TwinLock 7220 / 7260 BioPIN

Base - and Comfort Systems

Manual

DIN EN 1300
M 109317 High Security Lock Class EN B (TwinLock 7260 BioPIN)
M 109319 G High Security Lock Class EN C (TwinLock 7220 BioPIN)
G 108061 Hold-up Detector TwinXT
G 108062 Hold-up Detector TwinAlarm
G 106016 / G 106015 Blocking Device TwinXT Class C
G 105133 / G 102013 Ancillary Control Equipment (ACE) TwinAlarm (for IAS/BAS) Class C

Version 1.03B

Imprint

Copyright © März 2010 INSYS MICROELECTRONICS GmbH
Any duplication of this manual is prohibited. We appreciate comments and suggestions. All rights on this documentation and the devices are with INSYS MICROELECTRONICS GmbH Regensburg.

Trademarks

The use of a trademark not shown below is not an indication that it is freely available for use. Windows™ is a registered trademark of Microsoft Corporation.

Publisher

INSYS MICROELECTRONICS GmbH
Waffnergasse 8
93047 Regensburg, Germany

Contact

Phone: +49(0)941/58 692 22
Fax: +49(0)941//56 34 71
Email: insys@insys-security.de
Internet: http://www.insys-security.de

Table of Contents

1 General Information on This Manual 6

1.1 Content and Usage 6
1.2 General Qualification for Operating the System 6
1.3 Text Marks and Formatting 7
1.3.1 Safety Warnings 7
1.3.2 Icons and their Meaning 7
1.3.3 Operating Instructions 8

2 System Description 9

2.1 System 9
2.1.1 System Diagrams 10
2.1.2 System Components 17
2.1.2.1 Operating Unit FlatControl BioPIN 17
2.1.2.2 Lock TwinLock 17
2.1.2.3 Bus Distributor TwinConnect 17
2.1.2.4 Blocking Device TwinXT 18
2.1.2.5 ACE TwinAlarm 18
2.1.2.6 Optional Accessories: Chip Cards TwinCard 19
2.1.2.7 Survey: Codes in the System 20
2.2 Functions Overview 21
2.2.1 Standard Functions 21
2.2.2 Setting Functions with TwinComm USB 23
2.3 Intended Use 24

3 Operation 25

3.1 Basics 25
3.1.1 The System Status 26
3.2 Configuration via Optional Software TwinComm USB 27
3.3 Authorising the Users 27
3.3.1 Boxes of the User Matrix 29
3.4 Menu Navigation at Operating Unit FlatControl 30
3.5 PIN Codes 31
3.5.1 Types and Numbers of PIN Codes in Every Lock 31
3.5.2 Entering PIN Code 32
3.6 Code Cards 32
3.6.1 Code Card TwinCard code access 32
3.6.2 Inserting a Chip Card into the Operating Unit 32
3.7 Fingerprint Codes 33
3.8 Operation with CIT Function Selected 34
3.9 Opening and Closing 34
3.9.1 Opening a Lock with PIN Code 35
3.9.2 Opening a Lock with a Code Card 35
3.9.3 Entering Fingerprint Code and Opening a Lock 36
3.9.4 Triggering Silent Alarm When Opening a Lock 37
3.9.5 Opening a Lock with Dual Code 38
3.9.6 Opening a Lock with Timed Unlocking Delay 39
3.9.7 Opening with Timed Delay and Release Time 39
3.9.8 Opening Locks with Parallel Code 40
3.9.9 Disarming a Burglar Alarm System (BAS) 41

3.9.10 Closing a Lock ... 41
3.9.11 Closing a Lock with Code Input ... 41
3.9.12 Closing a Lock Automatically with the Door Switch ... 42
3.9.13 Setting / Arming a Burglar Alarm System (BAS) ... 42

3.10 Programming System Settings ... 43
3.10.1 Setting the Date and the Time of Day ... 43
3.10.2 Switching On / Off TwinXT or TwinAlarm ... 44
3.10.3 Setting the CIT Function (2 Groups of Users) ... 44
3.10.4 Exporting the Protocol (TwinComm USB) ... 45
3.10.5 Displaying / Printing the Protocol (TwinComm USB) ... 45
3.10.6 Importing the Configuration ... 46
3.10.7 Configuration Import: Error Messages ... 47
3.10.8 Exporting the Configuration (TwinComm USB) ... 49
3.10.9 Selecting a Language ... 49
3.10.10 Importing a Language ... 50

3.11 Administrating Users ... 51
3.11.1 Changing the System Manager Code ... 51
3.11.2 Changing the Master Code / CIT Master Code ... 52
3.11.3 Registering PIN Code for Users / Operators ... 53
3.11.4 Changing a PIN Code ... 54
3.11.5 Deregistering PIN Code ... 55
3.11.6 PIN Code User Display ... 56
3.11.7 Registering a Code Card ... 57
3.11.8 Deregistering a Code Card ... 58
3.11.9 Code Card User Display ... 59
3.11.10 Fingerprint: Survey ... 60
3.11.11 Fingerprint: Scan Test ... 61
3.11.12 Fingerprint: Determining Min. Minutiae ... 62
3.11.13 Fingerprint: Image Quality ... 63
3.11.14 Fingerprint: Security Level ... 64
3.11.15 Registering Fingerprint Code ... 65
3.11.16 Deregistering Fingerprint Code ... 66
3.11.17 Fingerprint User Display ... 67

3.12 Service ... 69
3.12.1 Supplying Power in Case of Power Breakdown ... 69
3.12.2 Displaying Status / Info about the System ... 69
3.12.3 Service Reset ... 70
3.12.4 Motor Service ... 72
3.12.5 Registering a New Lock ... 73
3.12.5.1 Additional New Lock ... 73
3.12.5.2 Changing a Lock ... 74
3.12.6 Locking the System despite Defect Bolt Work Contact ... 75
3.12.7 Fingerprint Status / Info ... 75
3.12.8 Fingerprint: Displaying / Modifying Temperature ... 76

4 Cleaning ... 76
5 Trouble Shooting ... 77
5.1 Error Messages ... 77
6 Support ... 84
7 Disposal ... 84
8 Glossary ... 85
9 Appendix ... 94

9.1 Index of Keywords 94
9.2 Table of Figures 96
9.3 Document Revision History 96
9.4 Notes 97

1 General Information on This Manual

1.1 Content and Usage

This manual contains information on operation, configuration and maintenance of the electronic high-security lock system TwinLock 7220 / 7260 BioPIN. Its purpose is to assist you in configuring and handling the system.

The manual describes the procedures of the systems approved to comply with VdS-class 2 standards (TwinLock 7260 BioPIN) and VdS class 3 standards (TwinLock 7220 BioPIN) and informs about the system settings. VdS Schadenverhütung GmbH is a company of the German Insurance Association, which evaluates security products.

For information on assembly and installation, see the Assembly Instructions, a separate document.

See the quick reference guide for instructions on opening and closing procedures.

1.2 General Qualification for Operating the System

This manual is addressed to qualified and trained specialists mainly. Persons configuring and administrating system TwinLock BioPIN have to be capable of reading and understanding the manual in order to become acquainted with all procedures necessary to set, administrate and operate the system. They should be able to instruct users, help them and generally ensure safe and secure operation of the system TwinLock BioPIN.

1.3 Text Marks and Formatting

1.3.1 Safety Warnings

Danger

Imminent mortal danger / Danger of severe injuries / health hazard.
Consequences which might arise from not being aware of the danger.
Instructions on how to avoid the danger or remove its cause.

Warning

Possibility of mortal danger / Danger of severe injuries / health hazard.
Consequences which might arise from not being aware of the danger.
Instructions on how to avoid the danger or remove its cause.

Caution

Danger of getting injured.
Consequences which might arise from not being aware of the danger.
Instructions on how to avoid the danger or remove its cause.

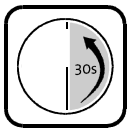
Caution

Danger of property damage.
Consequences which might arise from not being aware of the danger.
Instructions on how to avoid the danger or remove its cause.

Note

No warning but additional information.
Background information / hints.

1.3.2 Icons and their Meaning



Use the operating unit FlatControl.
After 30 seconds without operator input FlatControl switches to idle mode.

Tools are required.

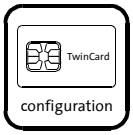
PIN code for operators is required.

Master code, PIN code for the master of the lock is required.

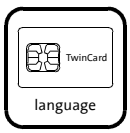
PIN code for the system manager code (manager code of lock 1) is required.

Fingerprint code for operators is required.

The optional chip card TwinCard code access is required.



The optional chip card TwinCard configuration II is required.



The optional chip card TwinCard language is required.

Icons for unprotected / protected premises in illustrations.

1.3.3 Operating Instructions

Unmarked text following a headline of a paragraph with operating instructions contains information, which may be worth considering before performing the operating procedures described. Such text does not contain safety instructions.

Take Text beginning with 'Take' contains information on tools or other things you should use in order to be able to perform the operating procedure successfully. Also take note of the icons (see above).

Settings Text beginning with 'Settings' contains preconditions necessary for a successful performance of the operating procedure.

1. Text, which looks like this, asks you to perform a task. The text may contain names of `Keyboard keys` and `Display Text` of the display of the operating unit.

   Text formatted like this contains mostly information on changes, which have been caused because you have performed a step of an operating instruction.

Text formatted like this closing a paragraph with operating instructions indicates that you have carried out the operating procedure successfully and achieved the objective.

2 System Description

2.1 System

TwinLock BioPIN is a modularly designed electronic high-security lock system. All parts important for security are fully redundant which ensures resilience.
With TwinLock BioPIN you can administrate, control and perform opening and locking procedures for doors used mainly in financial institutions of all kinds.
By using TwinLock BioPIN, you ensure the security of money and other precious items inside safes and similar containers for the storage of precious goods.

Authorised persons can open and lock the containers according to freely definable regulations in their daily routine. You can operate the system with two groups of users completely independent of each other like the staff of a bank and the staff of a company offering armoured car services.

There are two main types of the system:

- Base System 1.1, 2.1 and 3.2 (with TwinXT)
- Comfort System 1 and Comfort System 2 (with TwinAlarm)

The first number to follow the system name indicates the number of locks in the system. The second number indicates the number of blocking devices TwinXT, which come with Base Systems only.

Examples:
Base System 2.1 comes with 2 locks and 1 blocking device TwinXT.
Comfort System 1 comes with 1 lock and 1 ACE switching element TwinAlarm.

Every system contains an operating unit FlatControl, at least one lock TwinLock and a field bus distributor TwinConnect, which connects the components. All systems come with an Instruction Manual CD.

Comfort Systems contain 1 switching element TwinAlarm each.

Base Systems contain up to 2 blocking devices TwinXT each.

2.1.1 System Diagrams

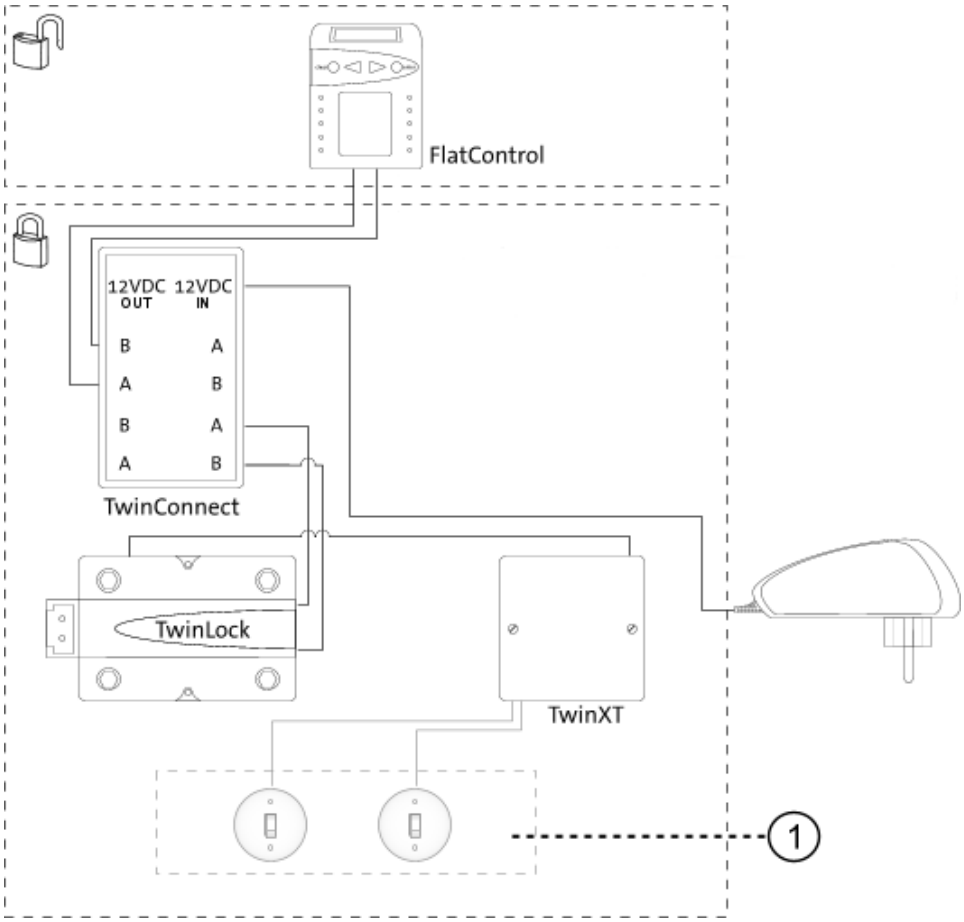


Fig. 1: System architecture of Base System 1.1

1) Optional bolt mechanism switch and release (enable) switch for lock TwinLock

Base System 1.1 consists of an operating unit FlatControl and a power supply outside the protected premises and one lock TwinLock, one bus distributor TwinConnect and one blocking element TwinXT inside the protected premises.

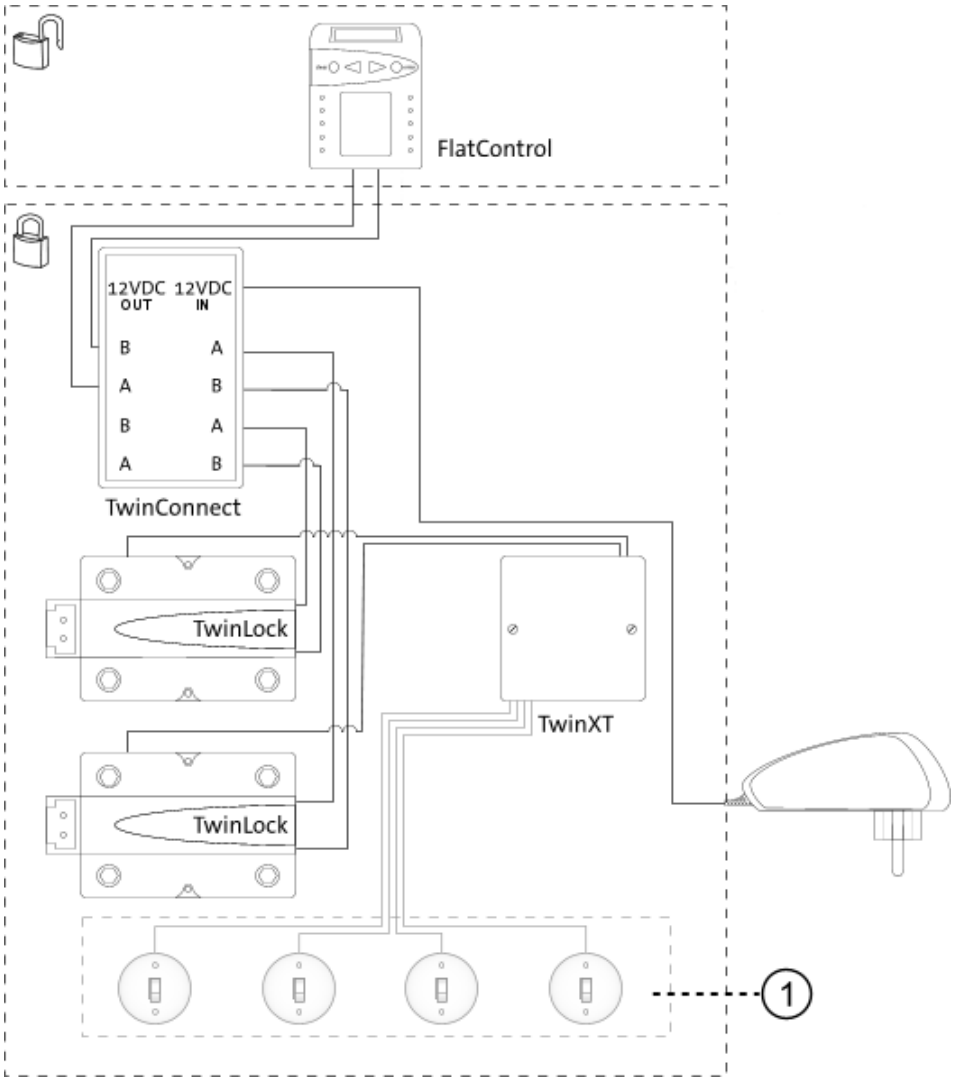


Fig. 2: System architecture of Base System 2.1

1) Optional bolt mechanism switches and release (enable) switches for locks TwinLock

Base System 2.1 features two locks inside the protected premises. All other components are the same as those of Base System 1.1.

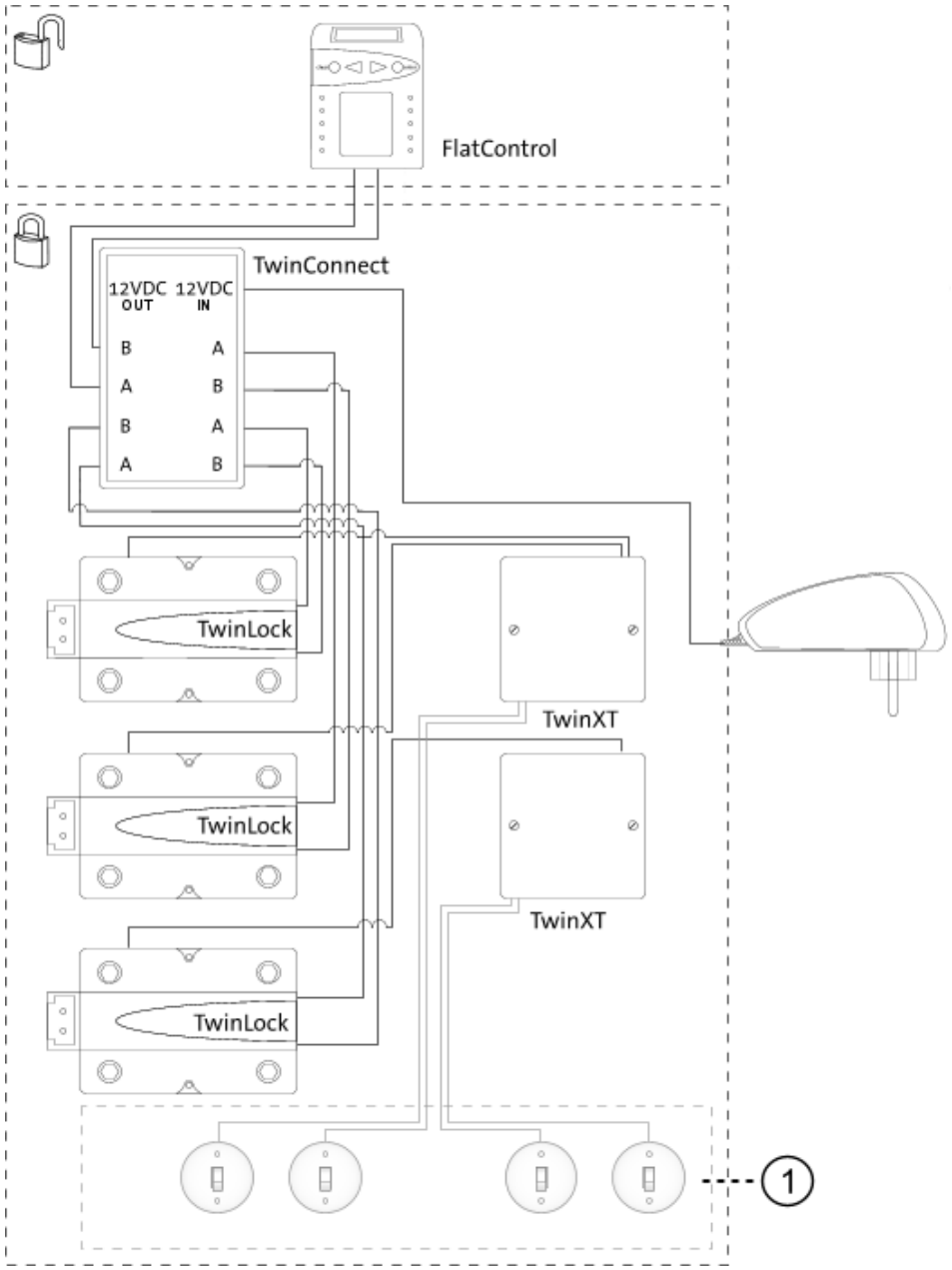


Fig. 3: System architecture of Base System 3.2

1) Optional bolt mechanism switches and release (enable) switches for locks TwinLock

Base System 3.2 features three locks and two blocking devices TwinXT inside the protected premises. All other components are the same as the ones of Base System 1.1.

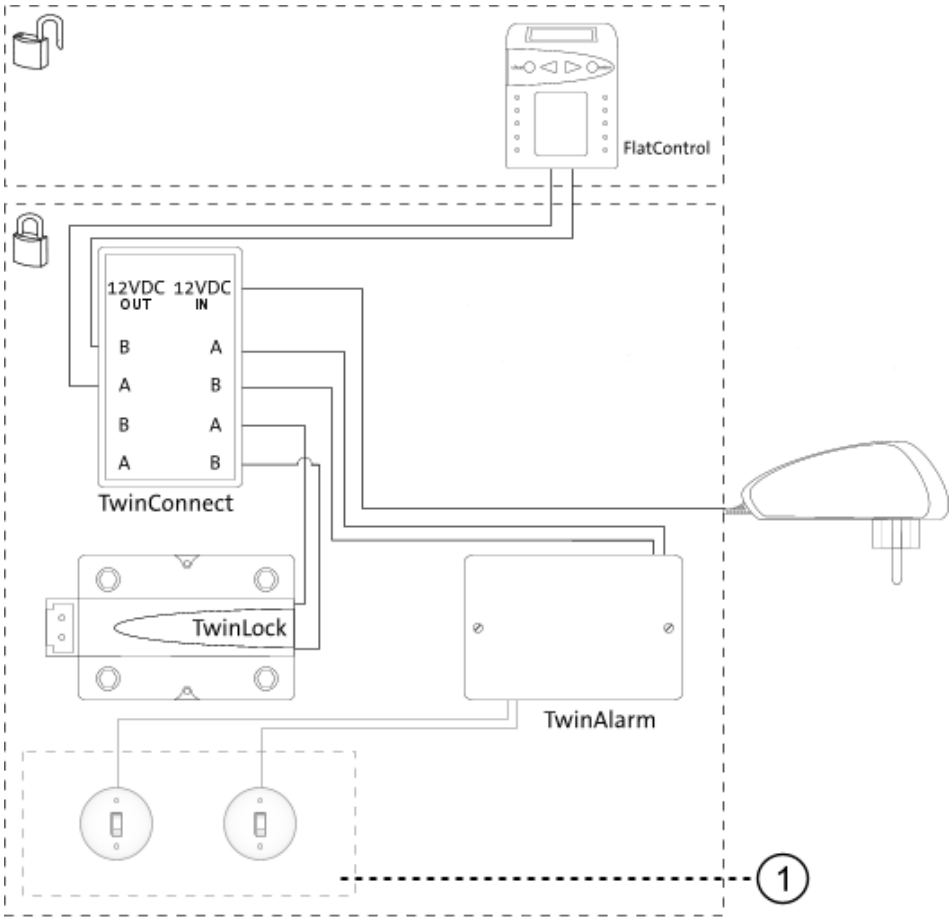


Fig. 4: System architecture of Comfort System 1 without BAS

1) Optional bolt mechanism switch and switch for timer program suspension for lock TwinLock

Comfort System 1 consists of an operating unit FlatControl and a power supply outside the protected premises and a lock TwinLock, a bus distributor TwinConnect and an ACE switching element TwinAlarm within the protected premises.

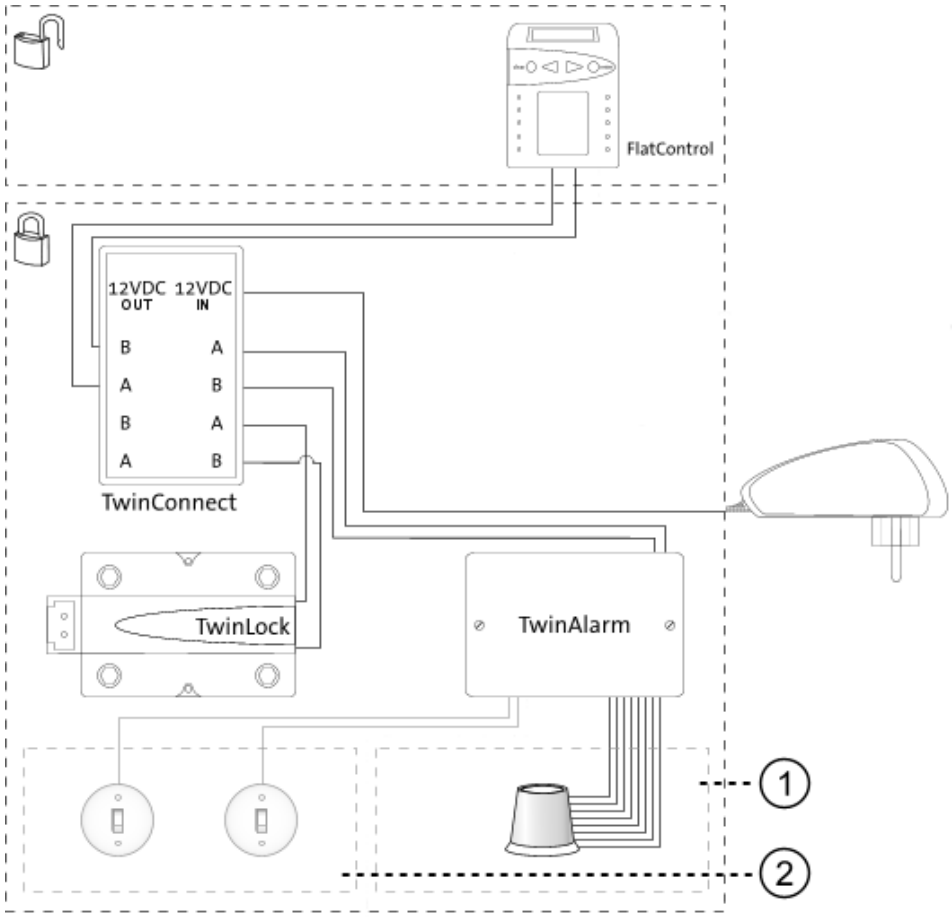


Fig. 5: System architecture of Comfort System 1 with BAS

1) Burglar Alarm System (BAS) with input (Alarm contact, state contact, Arming) from ACE unit TwinAlarm and output (BAS-Ready, Disarm-Block, Acknowledgement, Release – No release, Power supply) to unit TwinAlarm

2) Optional bolt mechanism switch and switch for timer program suspension for lock TwinLock

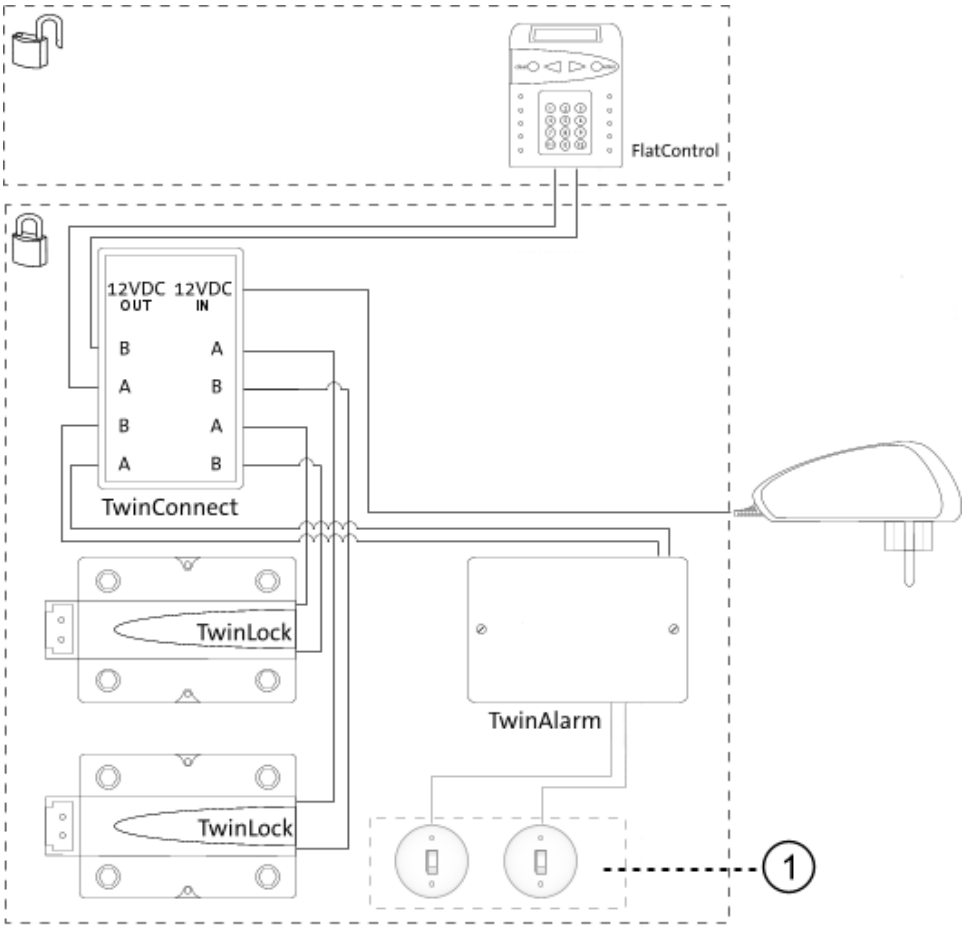


Fig. 6: System architecture of Comfort System 2 without BAS

1) Optional bolt mechanism switch and switch for timer program suspension for locks TwinLock

Comfort System 2 features two locks inside the protected premises. All other components are the same as those of Comfort System 1.

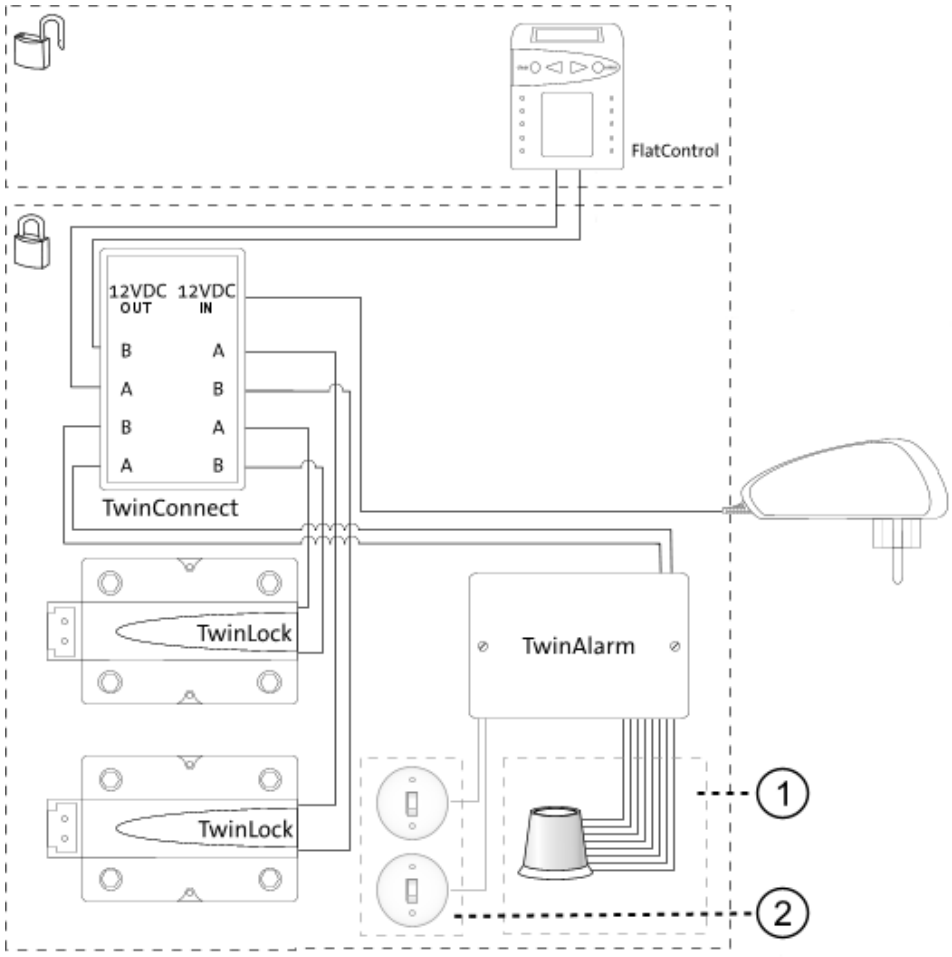


Fig. 7: System architecture of Comfort System 2 with BAS

1) Burglar Alarm System (BAS) with input (Alarm contact, state contact, Arming) from ACE unit TwinAlarm and output (BAS-Ready, Disarm-Block, Acknowledgement, Release – No release, Power supply) to unit TwinAlarm
2) Optional bolt mechanism switch and switch for timer program suspension for the two locks TwinLock

2.1.2 System Components

2.1.2.1 Operating Unit FlatControl BioPIN

Fig. 8: Operating Unit FlatControl BioPIN

With operating unit FlatControl BioPIN, set and operate system TwinLock. The operating unit is located outside the protected premises of the system. A description of its control elements see in chapter 4, 'Operation'.

2.1.2.2 Lock TwinLock

Fig. 9: Lock TwinLock

Lock TwinLock locks and unlocks the safe / container for valuables. It is located inside the protected premises. You can connect up to three locks to one system.

2.1.2.3 Bus Distributor TwinConnect

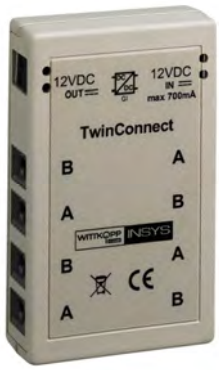


Fig. 10: Bus distributor TwinConnect

Via a redundant bus system the bus distributor TwinConnect connects the following system components with each other: per system 1 operating unit FlatControl, up to 3 locks TwinLock, 1 mains adapter, optionally 1-2 extension units TwinXT or 1 ancillary control equipment TwinAlarm. The bus distributor is located inside the protected premises.

2.1.2.4 Blocking Device TwinXT

Fig. 11: Blocking device TwinXT

Blocking device TwinXT inside the protected premises of the system is available as an extension unit for Base Systems only. With one unit TwinXT you can add 4 in- and 2 output contacts to the system. With these contacts up to 2 locks can be blocked / released independently and they can be equipped with bolt mechanism contacts. Additionally TwinXT provides a status- and an alarm contact for silent alarm.

2.1.2.5 ACE TwinAlarm

Fig. 12: Ancillary control equipment (ACE) TwinAlarm

Optional ACE TwinAlarm inside the safe / container for valuables connects the system with an optional burglar alarm system (BAS). It functions as distributor for the BAS (bolt-, door- and other contacts as well as resistance monitor). The electronic keys (chip cards) and the input signals of the BAS are evaluated in TwinAlarm.

2.1.2.6 Optional Accessories: Chip Cards TwinCard

Fig. 13: Icon 'TwinCard code access'

Code card **TwinCard code access** is the protected, mobile medium for code transmission for the users of the TwinLock system. As an alternative, code can also be entered manually.
In order to empower users to open locks with chip card, the system manager has to authorise them via user matrix and the 'lock master' has to register the chip card at the lock.

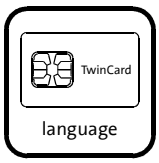


Fig. 14: Icon 'TwinCard language'

TwinCard language is an optional chip card for language import (DE, EN etc).

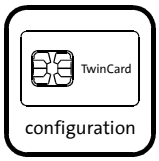


Fig. 15: Icon 'TwinCard configuration II'

TwinCard configuration II is an optional chip card for configuring the system and for the export of the system protocol. The protocols can be exported, displayed and saved for future reference. With the optional software TwinComm USB, the lock system can be configured via chip card. Configuration data can be saved.

2.1.2.7 Survey: Codes in the System

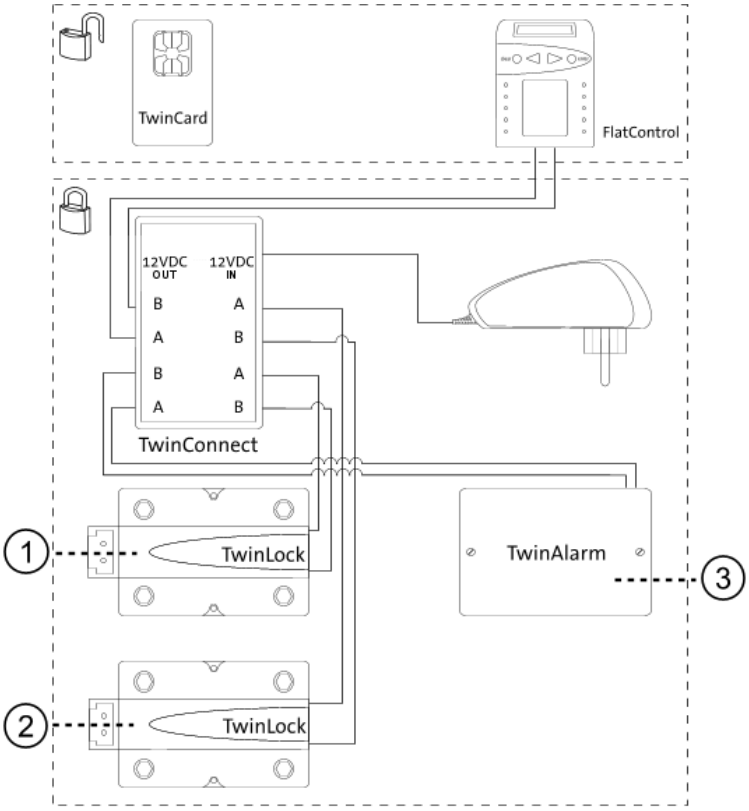


Fig. 16: Survey: codes in the system

1) **Lock 1**: mnemonic codes:
1 system manager code (manager code of lock 1)
1 master code
99 PIN codes for users (operators)

2) **Lock 2**: mnemonic codes:
1 master code
99 PIN codes for users (operators)

3) **TwinAlarm**: physical codes:
1 master code
PIN-Codes for users (operators)

Additionally there are physical codes saved on chip cards and encrypted fingerprint data (biometric codes).

Caution

With Comfort Systems: If PIN codes for users are registered at lock 1 before TwinAlarm is installed and activated, these PIN codes will not be saved in TwinAlarm. Users (operators) cannot arm and disarm the burglar alarm system with these PIN codes.
Make sure TwinAlarm is installed and activated before you register PIN codes for users at lock 1.

2.2 Functions Overview

2.2.1 Standard Functions

Depending on the kind and the version of system TwinLock BioPIN, all or a part of the functions listed incomprehensively on this and the following page can be set before or after the installation. Some of the settings can also be modified or changed at any time with operating unit FlatControl BioPIN.

Open and Close

Menu driven opening and closing processes
Menu driven administration and setting
Opening with code card and / or PIN code and / or fingerprint code
Opening with parallel code (2-lock-system) / dual code (4-eyes principle)
Automatic closing via door switch
Closing with chip card / code entry / without code of any kind
Quick open code / override code
Rigid order of opening / closing selectable

Code administration

1 preset system manager code, which can be changed
1 preset master code per lock
99 PIN codes for users at every lock, which can be set and changed
Per lock 10 fingerprint codes per user (for 100 users)
Display user status
99 alarm users
Alarm user status display
Parallel code
Quick open code (Override code for opening)
Selectable rigid order of lock opening (forced sequence)
Dual code (4-eyes code)
Protection against manipulation of code

Time related functions

Delays triggered by alarm and suspicion of attempt at sabotage
Silent alarm
Display of date and time
Automatic switching to / from Daylight Saving Time in spring / autumn
Release time
Opening delay
Special days
Part lock time
Weekly program
Timer program suspension

Comfort functions

Display backlighting
Self-diagnosis
Monitoring of voltage

Service functions

Protocols with entries of up to 3000 single processes to trace back
Im- / export of system configuration via chip card
Selectable language
System status display
Reset of system components
Display of versions of components
Register / de-register components
Motor test, one-step operation
System line freely programmable
Emergency power supply in case of power breakdown

TwinAlarm functions and burglar alarm system connection (optional)

Ancillary control equipment TwinAlarm ON / OFF
Connection to burglar alarm system (BAS)
Arming / Disarming of BAS manually or via chip card
Silent alarm
1 Status contact (relay)
1 Release contact (potential-free)
1 Bolt mechanism contact (potential-free)
Sockets for 2more bolt work - and door contacts for each lock
Extensible anti tamper loop
Surface protection
4 Door contacts
Override codes in order to suspend blocked periods / timer programs
Elements to be used for resistance monitoring

2.2.2 Setting Functions with TwinComm USB

TwinComm USB is software with which parameters of system TwinLock BioPIN can be set. It does not come with system TwinLock automatically. The following functions can be set with the software TwinComm USB:

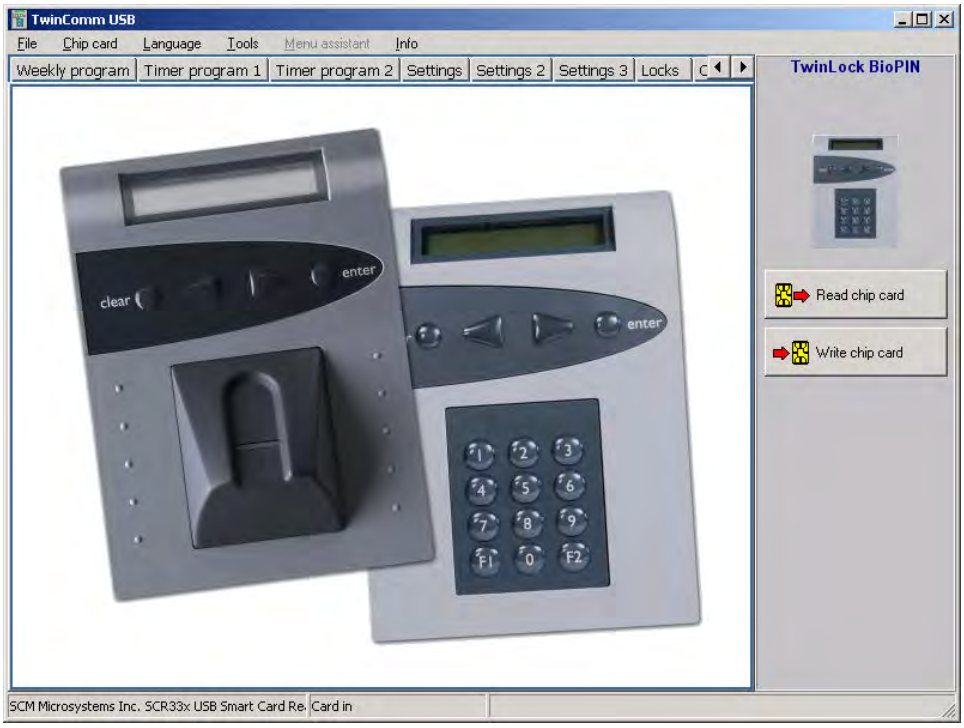


Fig. 17: PC software TwinComm USB (accessory)

General Settings

Automatic clock change to / from daylight saving time ON / OFF
Setting of battery warning signal for low voltage (optional)
Evaluation of the protocol
Programming of the 16 digit system headline

Open and Close

Dual code according to 4-eyes principle ON / OFF
Parallel code ON / OFF
Authorisation to open locks even while timer programs are active can be set for selected users
Forced sequence ON / OFF
Manual closing with code input ON / OFF
Automatic closing with door switch ON / OFF
Silent alarm, with or without opening delay ON / OFF
Code validity expiration adjustable
Open door monitoring adjustable
Time span between opening of lock 1 and lock 2 adjustable
Arming / disarming of a burglar alarm system (BAS)

Timer Programs

Opening delay adjustable (0-99 min.)
Release time adjustable (0-99 min.)
5 weekly programs for each day of the week
Special days program
3 Part lock time periods per weekday
3 Blocked - / Open periods

Administration functions

Easy system configuration
Blocking device TwinXT ON / OFF
Ancillary control equipment TwinAlarm ON / OFF
Selected users can be authorised to arm burglar alarm system
Survey of all parameters
Display of protocol
Display of customer data
User matrix with individual authorisation can be defined
Additional, independent CIT user range administrated separately
General and individually adjusted minimal requirements for fingerprint
Display of service phone number along with error message display

2.3 Intended Use

Warning

Danger of locking persons in.
Mortal danger due to possible lack of air / food.
Before closing a lock make sure that nobody is inside the container / room you are about to lock.

Use the high-security electronic lock system TwinLock BioPIN for opening and closing safes / containers for valuables and for the administration of the opening, and closing procedures only.

3 Operation

3.1 Basics

With operating unit FlatControl BioPIN set and operate system TwinLock BioPIN.

Additional settings can be made with the optional software TwinComm USB, if available. See the separate manual of TwinComm USB for information on how to how alter settings with the PC software.

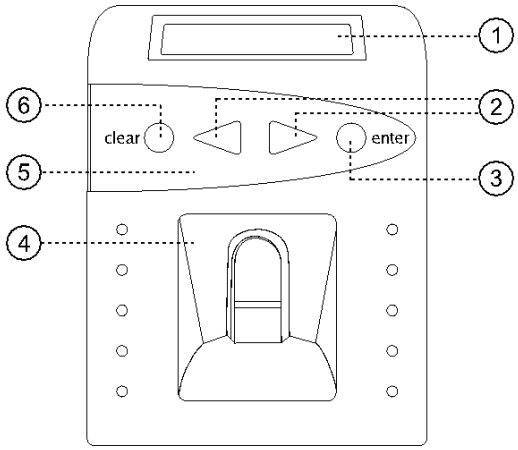


Fig. 18: Operating unit FlatControl BioPIN

1) 2-line alphanumeric display with lighting;
after activation the system menu with definable text in the first line and date / time in the second line is on display:

```
TwinLock BioPIN
Mi 10.02.10 08:30
```

2) Menu keys < and > for menu navigation to the previously displayed (<) / to the following (>) menu item and to select input
3) `Enter-key` for affirming / entering the selected menu item / input value
4) Finger guiding with fingerprint sensor
5) Menu keypad
6) `Clear-key` in order to cancel:
press and release -> selects the menu displayed previously
during code input -> undoes entering a number
press and hold 3 sec. -> selects the system menu

The displayed text will be displayed flashing after about 30 seconds without operator input. If the operator still does not enter anything, the system menu will be displayed. After that, the display will turn blank. You can activate the display by pressing any key.

A slot for chip cards is at the bottom of the operating unit.

3.1.1 The System Status

System settings can be modified and changed when the system is unlocked.
Only the menus `Open`, `Close` and `Status / Info` are on display at the operating unit when the system is locked.

In order to unlock the system,
- open lock 1 (with option 'Forced sequence' off [FS off]) – or
- open all locks (with option 'Forced sequence' on [FS on]).

With option 'Forced sequence' activated, users cannot select which lock of a system with 2 or 3 locks they open or close. Also see the Glossary.

System States:

Unlocked: Lock 1 ('Forced sequence' off [FS off]) / all locks (with FS on) open, all menus on display, system settings can be modified.

Partly locked: at least one lock open and one lock closed (with FS only), restricted menu display, system settings cannot be modified.

Locked: Lock 1 (with FS off) / all locks (with FS on) closed, restricted menu display, opening and emergency functions available, system settings cannot be modified.

The state of the system depends on whether option 'Forced sequence' (FS) has been set via software TwinComm USB during configuration:

System status with 'Forced sequence' OFF
Unlocked / not protected, when lock 1 is open. Display of all menus.
With this setting there is no state 'Partly blocked'. .
Locked, when lock 1 is locked. Menu display restricted.

System status with 'Forced sequence' ON
Unlocked / not secure, when all locks are open.
Partly blocked when at least one lock is closed and another lock is open.
Locked, when all locks are locked.

Status contact of TwinAlarm / TwinXT (optional)
Only with systems with TwinXT / TwinAlarm:
Contact in state 'open' / 'closed', when lock 1 is open / closed.

System signal of status contact of TwinAlarm/TwinXT (optional)
Only with systems with TwinXT / TwinAlarm:
System signal indicates 'open' / 'closed', when lock 1 is open / closed.

3.2 Configuration via Optional Software TwinComm USB

System TwinLock BioPIN can be operated without software TwinComm USB. With this PC software some additional features are available.

The optional configuration set TwinComm USB simplifies the configuration and enables the installation of timer programs and the evaluation of the protocol. Additionally the authorisation of users (operators) can be modified flexibly.

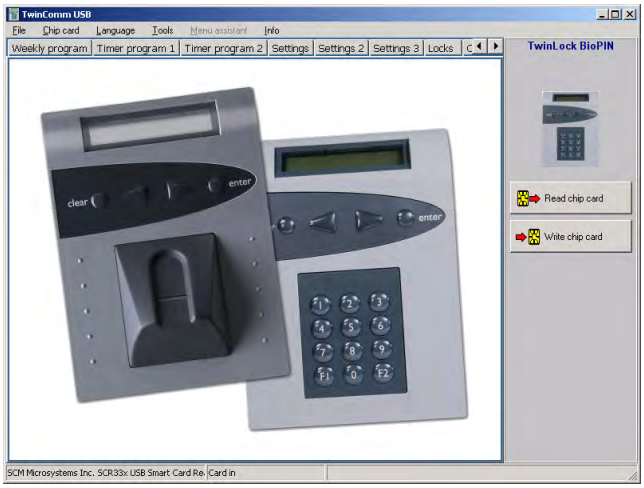


Fig. 19: Start page of PC software TwinComm USB (accessory)

The system administrator enters configuration data via the graphical user interface of software TwinComm USB.

Data are transmitted to and from system TwinLock via chip card TwinCard configuration II with the help of the function `Import / Export` at the operating unit FlatControl and an optional card reader / -writer device at the PC.

3.3 Authorising the Users

The system manager defines the authorisation of users in a matrix by ticking (AE: checking) boxes for them (see illustration below; description of the boxes see next section. The authorisation is set after the installation of the system. It can be modified and changed at any time via optional software TwinComm USB.

In order to make the defined settings valid in the lock system, the system manager imports the configuration from software TwinComm USB into system TwinLock.

An operator / user can open a lock in case she / he has been authorised to do so and in case the lock master (bearer of the master code of the lock) has registered

- PIN code or / and
- Code card or / and
- Fingerprint code at the lock for the user.

If an operator (user) is not authorised to carry out a certain procedure, the message `Authorisation` will be displayed on the operating unit. If `Authorisation | PIN code` is on display, for example, the operator has not been authorised to enter PIN code. In that case, the operator should contact the system manager.

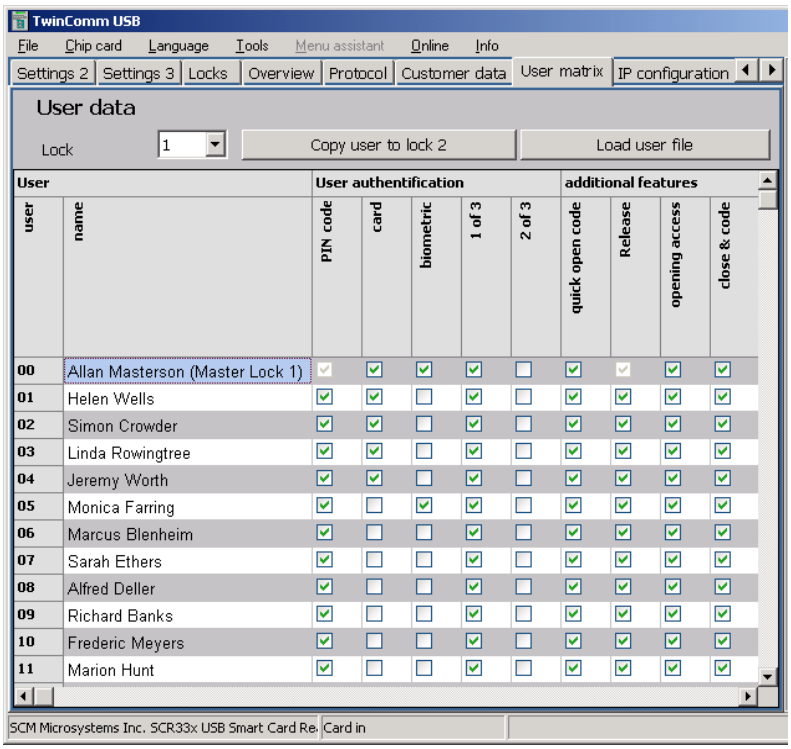


Fig. 20: Section of user matrix in TwinComm USB

If for certain users the box **Release** is not ticked [AE: checked] in the user matrix, these users will not have any rights and no function will be available for them.

Caution

Users cannot open locks in case they have not been authorized sufficiently.
Tick off the boxes for authorisation only after reading this manual or after having consulted an expert on system TwinLock. If necessary, tick further boxes like **Card** for code cards, for example.

Authorization for opening locks via entering PIN code:
The system manager ticks [AE: checks] boxes **PIN code**, **Release**, **Open locks** and, if a burglar - / intruder alarm system (BAS / IAS) is connected, also **Disarm** for the user.

Authorization for opening locks via inserting code card:
The system manager ticks boxes **Card**, **Release**, **Open locks** and, if a BAS / IAS is connected, also **Disarm** for the user.

Authorization for opening locks via entering fingerprint code:
Nobody can open a lock by entering fingerprint code only.
The system manager ticks boxes **Fingerprint**, **Release**, **Open locks** and, if a BAS / IAS is connected, also **Disarm** for the user. Additionally the user has to be authorised to enter PIN code or insert a code card.

The system manager also sets whether users can choose between entering PIN code, inserting a code card and entering fingerprint code (see following section, boxes **1 0f 3** and **2 of 3**).

3.3.1 Boxes of the User Matrix

In order to be able to perform operational tasks, an operator / user has to be authorised to do so. Users and lock master (= user 00) can be authorised to open locks, for example, by the system manager, who cannot open locks himself.

See the following list of all boxes, which the system manager can tick [AE: check] for all or for selected users:

Boxes to Enable User Authentication

PIN code	Authorisation to enter PIN code
Card	Authorisation to insert a code card
Fingerprint	Authorisation to enter biometric data (NOTE: Entering fingerprint code alone does not open locks)
1 of 3	Authorisation to choose a way of code input
2 of 3	Authorisation to choose two ways of three possible ways of code input

Boxes to Activate Additional Features

Quick open code	Authorisation to open locks even when they are blocked (override active timer programs)
Release	General authorisation to enter code
Open locks	Authorisation to open locks
Close	Authorisation to close locks
Service	Authorisation to export the protocol
2-eyes	Authorisation to open / close alone even with 4-eyes principle activated

Caution

With systems with a burglar alarm system (BAS), users can open locks only in case the box 'Disarm' is ticked for them.
Do not tick off box **Disarm** for users supposed to open locks. This also applies to the lock master.

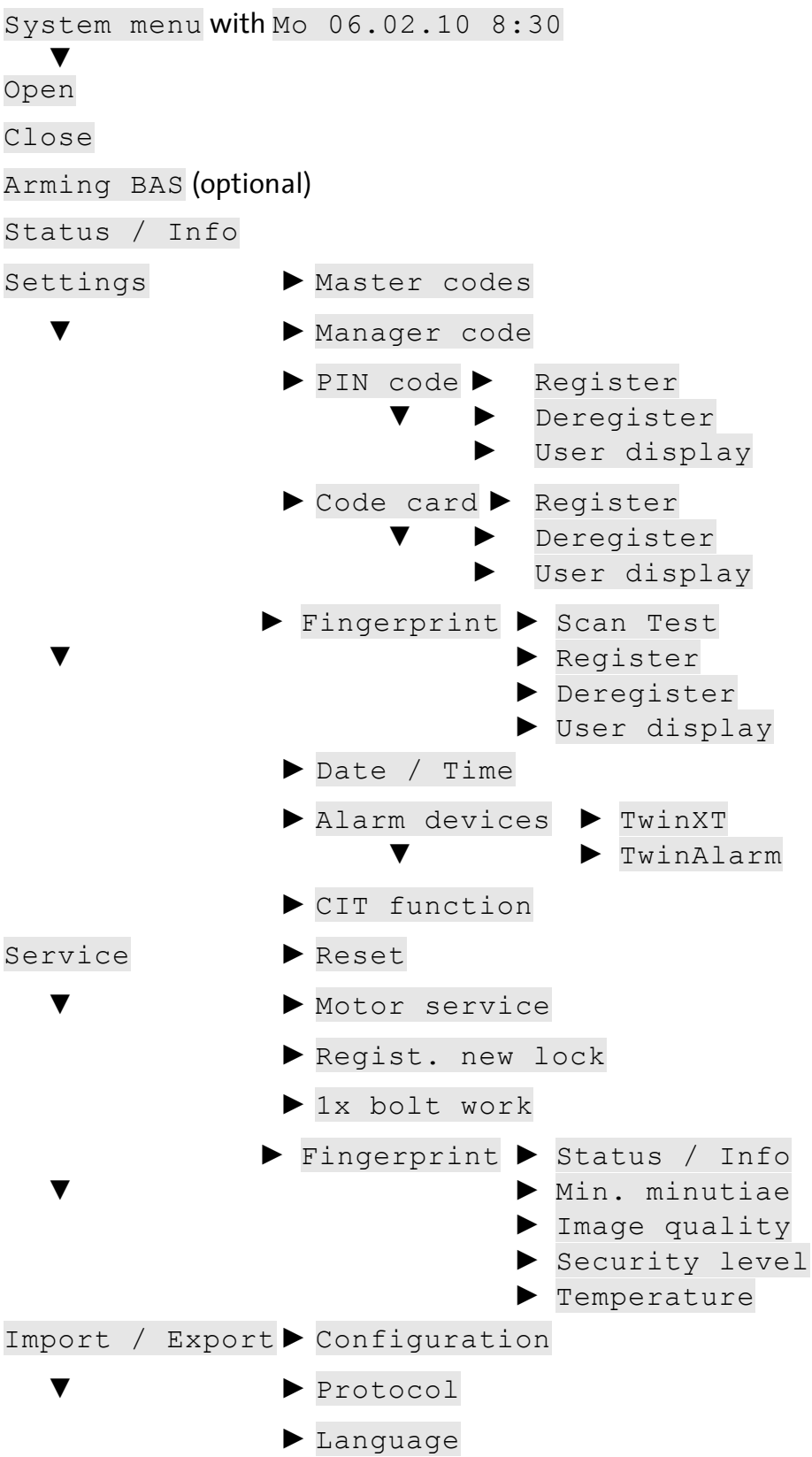
Disarm	Authorisation to disarm an optional burglar alarm system

Boxes to Assign Weekly Programs to Users

WP1 – WP5	If boxes are ticked [AE: checked], the Weekly Programs selected are assigned to the selected users and these can open during opening periods defined in the Weekly Program.

3.4 Menu Navigation at Operating Unit FlatControl

(with system unlocked)



3.5 PIN Codes

Caution

The system is not protected with ex works versions of system manager – and master code.
Danger of unauthorised opening.
Due to security reasons, please change the ex works versions of codes as soon as possible.

Caution

Codes consisting of numbers that correspond to personal data like birthday dates might be guessed at.
Danger of unauthorised opening.
Avoid using numbers, which might be guessed at by people with access to your personal data.

Caution

If you register PIN code at a lock but cannot repeat entering it, the lock cannot be opened.
Danger of unsuccessful attempts at opening.
Test and repeat entering new PIN codes with the storage unit open and store the codes in a secure place

3.5.1 Types and Numbers of PIN Codes in Every Lock

- 1 system manager code (without authorisation to open the lock)
- 1 master code (with authorisation to open the lock)
- 99 user PIN codes (also with optional authorisation to open the lock, see section 'Authorising the Users' in this chapter).

The whole system can be configured with the **manager code** of lock no.1. This code also is called **system manager code**, system code in short, and its bearer is called system manager.

With the **master code** of a lock the PIN codes of the operators / users can be registered and deregistered. The code bearer is called the lock master, who can optionally be authorised to open the lock by the system manager. system–, manager- and master codes cannot be deregistered or deleted.

With every operator / user **PIN code** registered at a lock by the lock master, users who have been authorised by the system manager can open the lock.

PIN codes for users are not programmed ex works, but activated. Via the user matrix of TwinComm USB the individual authorisation of users is defined. The PIN codes can be programmed / registered and deregistered by the lock master. Every user can change his PIN code and depending on his authorisation can open the lock and close it with PIN code input, if necessary.

The number of digits of a PIN code (for users, lock master, manager and system manager) depends upon the VdS class of the system. VdS Schadenverhütung (= VdS loss prevention) is an independent, accredited and notified testing and certification institution for physical and electronic protection against intrusion.

The **VdS class** of TwinLock BioPIN can be displayed via menu `Status / Info` at the operating unit.

TwinLock systems of VdS class 2 contain locks type TwinLock 7260 only, systems of class 3 contain locks type TwinLock 7220.

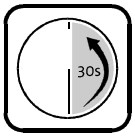
With systems of VdS class 3, every PIN code consists of eight digits.
With systems of VdS class 2, every PIN code consists of six digits.

Ex Works Master- and System Manager Codes		
	Master	**System / Manager**
VdS class 2	123456 (user 00)	111111 (user 225)
VdS class 3	12345678 (user 00)	11111111 (user 225)

With systems 7220, VdS class 3, the master code, assigned to user no. 00, at all locks is '12345678' ex works. The manager code of a lock / the system manager code of lock no. 01, assigned to user no. 225, is '11111111' ex works.

With systems 7260, VdS class 2, the codes ex works are similar, see table above.

3.5.2 Entering PIN Code



All operators (users, managers and masters) enter their PIN code via menu keys.

Settings Boxes **PIN code**, **Release** and **Open locks** of the user matrix (TwinComm USB) have been activated for you. Your PIN code is registered at the lock.

1. Follow the steps of an instruction until code input is required.
   Before you enter code, among other things `0123456789` *is displayed and the cursor flashes in the place of a random digit.*
2. With keys < and > select a digit of your PIN code and confirm with `Enter`. In this way select the digits one by one.
   An asterisk is displayed instead of the digit entered: `Code: ***`. *After your input a following message is displayed like* `Please wait`*, for example.*
3. If necessary, perform further steps of the instruction.

You have entered PIN code successfully.

3.6 Code Cards

3.6.1 Code Card TwinCard code access

Optional **Code cards** (TwinCard code access) can be registered and deregistered by the lock – (and WTU-) masters only. At every lock, they can register a code card for every user. There may be up to 99 users at a lock. Ex works the card codes for user no. 01 – 99 are inactive. Also see paragraph 'Authorising the Users'.

3.6.2 Inserting a Chip Card into the Operating Unit

If authorised by the system manager (see 'Settings' below), a user / operator can open a lock with the optional chip card TwinCard code access (see 'Open a Lock with Code Card' in this chapter). With the optional chip card TwinCard configuration II the configuration can be transferred and protocol data can be exported. With TwinCard language the system manager can import languages.

Settings for TwinCard code access:
boxes **Card, Release** and **Open locks** at the user matrix have been ticked (AE: checked) for the user, the card is registered.

for TwinCard configuration II:
boxes **Release** and **Service** of the user matrix have been ticked for the user, the card is registered.

Take optional chip card TwinCard code access / - configuration II.

1. When `Insert card` is on display at the operating unit, insert a chip card TwinCard of the proper type into the card slot.
   Audibly the card clicks into place. The chip is inside the upper part of the card. You face the reverse side of the card.

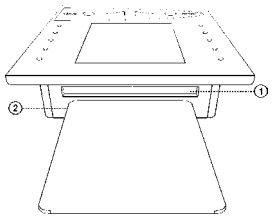


Fig. 21: Card and card slot of FlatControl BioPIN

1) Card slot of FlatControl
2) Chip card TwinCard (code access / configuration II / language)

2. Wait until `Remove card` is on display.

3. Remove the chip card from the operating unit.

You have successfully inserted the card and removed it again.

3.7 Fingerprint Codes

Fingerprint codes (max. 10 per user, for 99 users + 1 master per lock) can be registered and changed exclusively by the lock master and the users working together. These codes can be deregistered by the master only. Unlike the input of other kinds of code, the input of fingerprint code alone cannot trigger lock opening. A user has to enter at least one other kind of code as well. Also see ‘Authorise the Users’ above.

For further information on Fingerprint see the instructions in this chapter beginning with ‘Fingerprint: Survey’ and the Glossary at the end of the manual.

3.8 Operation with CIT Function Selected

Caution

Without an authorised CIT master with PIN code registered, the second user group (CIT user) cannot be administrated.
Authorise user no.99 with all rights required **before you activate the CIT function** (see paragraph 'Authorising the Users' and register code for user no.99 at the lock.

For users / operators, the operation is the same with or without the CIT function.

If option 'CIT' is activated (also see 'Activating the CIT function' in this chapter), the users of every lock will be split into two groups. The size of the groups can be defined via TwinComm USB (ex works: group 1 consists of users 01-50 with lock master and group 2 consists of users 51-98 with CIT master).
The lock master administrates the first group (users 01 to XX-1).
User 99, who turns CIT master, administrates the CIT users (user XX to 98).

Lock master and CIT master additionally select 'Master' / 'CIT master' before they enter code:

1. Follow the steps of an instruction until code input is required.
   Before code input is required from the master or the CIT master, `Code entry | User: Master` *is displayed.*

2. Confirm `Master` with `Enter` or with menu key < or > select `CIT master` and press key `Enter`.
   `CIT master` *or* `Master`, `Code entry`, `0123456789`, *as it may be, and* `Code:` *are displayed.*

3. Enter master- or WTU master code and, if necessary, perform further steps of the instruction.

You have successfully selected master / CIT master.

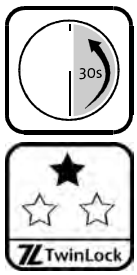
3.9 Opening and Closing

Caution

If a burglar alarm system (BAS) is connected to the system, no user can open lock 1 unless she / he is authorised to disarm the BAS.
In the user matrix of TwinComm USB, tick box **Disarm** for users, if a BAS is connected.

In order to unlock the system, open all locks or open lock 1 depending on the system settings. Also see paragraph 'The System Status'.

3.9.1 Opening a Lock with PIN Code



Settings Boxes **PIN code**, **Release**, **Open locks** and, if necessary, **Disarm** of the user matrix have been ticked (AE: checked) for the operator. The lock master has registered your PIN code at the lock.

1. Press key `Enter` and release it after a second.
   The system checks its status. Date and time are on display.

2. With key < or key > select `Open` and confirm with key `Enter`.
   When `Open` is not on display, the lock already is open.
   With 2 or 3 locks in the system, `Lock: 1` is on display, too.

3. If necessary, select the lock with key < or > and press `Enter` again.
   `Code entry | User: Master` is on display. If you confirm with `Enter`, `Master | PIN code` is on display and you can select `Code card` and open as master.

4. With < and > and `Enter` select your user number.
   `User no. | PIN code` is on display.

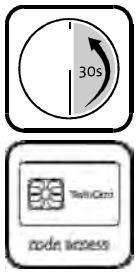
5. Confirm with `Enter`.
   `User no.`, `0123456789` and `Code:` are on display.
   Also see paragraph 'Entering PIN Code'.

6. Enter your PIN-Code with keys < and > and `Enter`.
   `Code entry` may be on display again. In this case, select `Code card` or `Fingerprint`. Also see the following instructions.

   For users who open with PIN code only, `Open| Please wait` is on display. The lock bolt is retracted. `Open | Lock open: no.` is on display, and, with all locks open, `System unlocked` is, too.

You have successfully opened the lock (either by entering PIN code or by additionally entering fingerprint code and / or inserting your code card).

3.9.2 Opening a Lock with a Code Card



Settings Boxes **Card**, **Release**, **Open locks** and, if necessary, **Disarm** of the user matrix (have been ticked (AE: checked) for you. The lock master has registered your code card at the lock.

Take the optional chip card TwinCard code access.

1. Press key `Enter` and release it after a second.
   The system checks its status. Date and time are on display.

2. With key < or key > select `Open` and confirm with key `Enter`.
   With 2 or 3 locks in the system, `Lock: 1` is on display, too.
   If all locks are open, menu `Open` cannot be selected.

3. If necessary, select the lock with key < or key > and press `Enter` again.
   `Code entry | User: Master` is on display. If you confirm with `Enter`, `Master | PIN code` is on display and you can select
   `Code card` and open as 'master'.

4. With < and > and `Enter` select your user number.
   `User no. | PIN code` is on display.

5. With < or > select `Code card` and press `Enter`.
   `User no. | Insert card` is on display.

6. Insert card TwinCard code access into card slot
   (see paragraph 'Inserting a Chip Card into the Operating Unit').
   `Reading Data` and afterwards `Remove card` are on display.

7. Remove the card.
   `Please wait`, afterwards `OK` and `User no. | PIN code` may be on display. In this case you can additionally enter PIN code and / or fingerprint code, if necessary.
   See 'Opening a Lock with PIN Code'.
   For users who open via Code card only, `Open| Please wait` is on display. The lock bolt is retracted. `Open | Lock open: No.` and, with all locks open, also `System unlocked` is on display.

You have successfully opened the lock (either by inserting your code card only or by entering PIN code or / and fingerprint code additionally).

3.9.3 Entering Fingerprint Code and Opening a Lock

Entering fingerprint code alone is not sufficient in order to trigger lock opening. See paragraph 'Authorise the Users' above. If you use a finger, which has been declared 'Alarm finger', silent alarm will be triggered.

Settings You have been authorised to enter **Fingerprint** code and together with the master of the lock, you have registered fingerprint code at the lock.

1. Press key `Enter` and release it immediately.
   The system checks its status. The display shows date and time.

2. With key < or key > select `Open` and confirm with key `Enter`.
   `Open` and, as the case may be, `Lock 1` are on display.

3. With key < or key > select the lock, if necessary, and press `Enter`.
   `Code entry | User: Master` is on display. If you confirm with `Enter`, `Master | PIN code` will be on display and you can open as 'Master'.

4. With < and > and `Enter` select your user number.
   `Code entry | PIN-Code` is on display.

5. With < or > select `Fingerprint` and `Enter`.
   `R. index finger` or another finger is on display (R= Right).

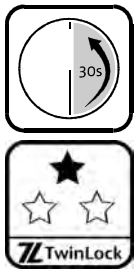
6. With < and > select the finger to be scanned and press `Enter`.
   `<<SCAN>>` is on display. As long as the angle brackets around '`SCAN`' are animated, fingers can be scanned. If you scan the Alarm finger in the next step and the system features this function, silent alarm will be triggered.

7. Put a finger already registered at the lock into the guide at the operating unit so that it touches the surface and steadily move it downwards.
   `Please wait` is on display and `OK`, `Code entry` and `PIN code`, as the case may be, and you can enter PIN code and / or insert your code card.

   In case the input of fingerprint code has been the final part of the authentication process, `Open | Please wait` is on display. The lock bolt is retracted. `Open | Lock open: no.` is on display.

You have entered fingerprint code successfully.

3.9.4 Triggering Silent Alarm When Opening a Lock



This is a way to send a message calling for help without being noticed doing so. The alarm can**not** be triggered **via Chip card**. With fingerprint code, scanning the 'Alarm finger' triggers silent alarm. When entering PIN code, trigger the alarm by carrying out the steps listed below.

Settings Boxes **PIN code**, **Release** and **Open locks** and **Disarm** of the user matrix have been ticked (AE: checked) for you. The lock master has registered your PIN code at the lock. Option 'Silent alarm' has been activated via software TwinComm USB.

Take an activated device TwinXT / TwinAlarm and a burglar (intruder) alarm system (BAS / IAS).

1. Press key `Enter` and release it after a second.
   The system checks its status. Date and time are on display.

2. With menu key < or > select `Open` and confirm with key `Enter`.
   With 2 or 3 locks in the system, `Lock: 1` is on display.

3. If necessary, select the lock with < or > and press `Enter` again.
   `Code entry | User: Master` is on display. If you confirm with `Enter`, `Master | PIN code` is on display and you open as 'master'.

4. With < and > and `Enter` select your user number.
   `User no. | PIN code` is on display.

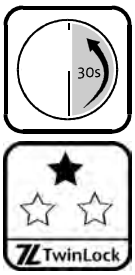
5. Confirm with `Enter`.
   `User Nr, 0123456789` and `Code:` are on display. Enter the code - here the alarm code. See paragraph 'Entering PIN Code'.

6. With < and > and `Enter` select all numbers of your code but the last one.

7. Instead of the last number ('8', for example) take its value (8) and add the value which has been set in TwinComm USB for 'Silent alarm' (ex works '1', value range 1-9) and confirm with `Enter`.
   If the result should turn out a two-digit number, instead of sum '11' enter 1, instead of '12' 2, instead of '13' 3 etc.
   The messages displayed and, if necessary, additional further opening procedures are the same as those of a standard opening process.

You have successfully triggered silent alarm.

3.9.5 Opening a Lock with Dual Code



Only if both participating operators carry out all kinds of authentication assigned to them, the lock will open.

Settings

On tab 'Settings' of TwinComm USB the option 'Dual code / 4-eyes (Opening)' is activated.

Boxes **PIN code** / **Card**, **Release** and **Open locks** and, if necessary, **Disarm** have been and **Single code** of the user matrix has not been ticked (AE: checked) for you.
The lock master has registered PIN code at the lock.

1. Press key `Enter` and release it immediately.
   The system checks its status. Date and time are on display.

2. With key < or key > select `Open` and confirm with key `Enter`.
   `Open` *is on display. With more than one lock,* `Lock: 1` *is on display, too.*

3. If necessary, select the lock with < or > and press `Enter` again.
   `Code entry &1 | Master` *is on display.*

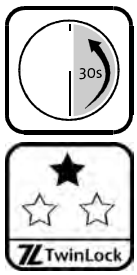
4. With < and > and `Enter` select your user number.
   `User no. | PIN code` *is on display.*

5. According to your user settings, with `Enter` select `PIN code` or with < and > and `Enter` select `Code card` or `Fingerprint` and carry on as usual when opening.
   See the instructions 'Opening a Lock...' at the beginning of this chapter. Another person is to perform the next step.
   `Code entry &2 | Master` *is on display.*

6. A second operator gives his authentication at the lock.
   See steps 4 and 5.
   `Open | Please wait` *is on display. The lock bolt retracts.*
   `Open | Lock open: No.` *is on display.*

Your colleague and you have successfully opened the lock with dual code.

3.9.6 Opening a Lock with Timed Unlocking Delay



Settings On tab 'Locks' of TwinComm USB, a value greater than zero has been set for 'Unlocking delay'.
Boxes **PIN code** / **Card** and / or **Fingerprint**, **Release** and **Opening access** and, if necessary, **Disarm** of the user matrix have been ticked (AE: checked) for you. Code has been registered at the lock.

1. Press key `Enter` and release it immediately.
   The system checks its status. Date and time are on display.

2. With key < or key > select `Open` and confirm with key `Enter`.
   `Open` *is on display. With more than one lock,* `Lock: 1` *is on display, too.*

3. If necessary, select the lock with menu key < or > and press `Enter` again.
   `Code entry | User: Master` *is on display.*

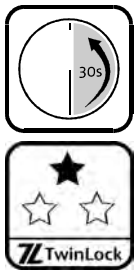
4. With < and > and `Enter` select your user number.
   `User no. | PIN code` *is on display.*

5. According to your user settings, with `Enter` select `PIN-Code` or with < and > and `Enter` select `Code card` or `Fingerprint` and carry on as usual when opening.
   See the instructions 'Open a Lock...' at the beginning of this chapter.
   `Open | Time: 00:00` *is on display. The first 2 numbers indicate the number of minutes; the last 2 numbers indicate the number of seconds.*

6. Wait until the 'Unlocking delay' ends.
   An acoustic signal indicates the end of the unlocking delay.
   `Open | Please wait` *is on display. The lock bolt retracts.*
   `Open | Lock open: no.` *is on display.*

You have successfully opened the lock.

3.9.7 Opening with Timed Delay and Release Time



This paragraph is a sequel of the last one.

Settings See the last paragraph. Additionally option 'Release time' in TwinComm USB is activated.

1. Perform steps 1-6 of the last paragraph and be prepared to enter code.
   An acoustic signal indicates the end of the delay. During the release time, which follows, an acoustic signal sounds every two seconds.
   `Code entry | Lock No.` *is displayed in case there are 2 or 3 locks in the system. If you do not enter anything before the release time ends, the system will abort the opening process.*

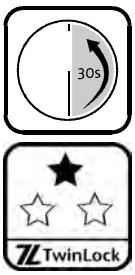
2. If necessary, select the lock with key < or key > and press `Enter`.
   `Code entry | Master` *is on display.*

3. With < and > and `Enter` select your user number.
   `User no. | PIN code` *is on display.*

4. Enter your PIN code and / or insert your code card.
   See step 5 of the last paragraph. `Open | Please wait` *is on display. The lock bolt retracts.* `Open | Lock open: no.` *is on display.*

You have successfully opened the lock.

3.9.8 Opening Locks with Parallel Code



The first operator opens lock 1, the second one opens lock 2 and a third one, as it may be, opens lock 3. All operators open according to their authorisation.

Settings Option 'Parallel code' (for systems with 2 / 3 locks only) is activated TwinComm USB. Boxes **Release**, **Opening access**, **PIN code**, / **Card** and / or **Fingerprint** and, if necessary, **Disarm** of the user matrix have been ticked (AE: checked) for you. The lock master has registered your PIN-Code / card at the lock.

1. Press key `Enter` and release it after a second.
   The system checks its status. Date and time are on display.

2. With menu key < or > select `Open` and confirm with key `Enter`.
   `Open` *is on display. With more than one lock,* `Lock: 1` *is on display, too.*

3. If necessary, select the lock with menu key < or > and press `Enter` again.
   `Code entry | Master` *is on display.*

4. With < and > and `Enter` select your user number.
   `User no. | PIN code` *is on display.*

5. With `Enter` select `PIN code` or with < or > and `Enter` `Code card` and open according to your user settings in the user matrix.
   See the instructions 'Open Lock ...' at the beginning of this chapter. Lock 1 opens. `Open | Lock open: 1` *is on display.*

6. Another operator carries out steps 1-5 at lock 2 and, if necessary, a third one does the same at lock 3.
   `Open | Please wait` *is on display. The lock bolt retracts.*
   `Open | Lock open: No.` *is on display.*

You have successfully opened the lock.

3.9.9 Disarming a Burglar Alarm System (BAS)

If operators are not authorised to disarm a BAS, they will not be able to open locks in case a BAS is connected and armed. Disarming takes place automatically with opening.

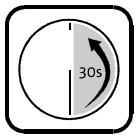
Settings Boxes **PIN code**, **Release** and **Opening access** and **Fingerprint** or **Card** and, if necessary, box **Disarm** of the user matrix have been ticked (AE: checked) for you. TwinAlarm and BAS are connected, TwinAlarm is activated, BAS is armed and all locks are closed. The lock master has registered your PIN-Code and your code card at the lock.

Take chip card TwinCard code access, if necessary.

- Enter your PIN code and additionally
  enter Fingerprint code or insert your code card.
  See the instructions for opening a lock at the beginning of the chapter. The code card is TwinCard code access.

You have opened the lock and by doing so successfully disarmed the BAS.

3.9.10 Closing a Lock



Settings The bolt work contact does not actively prevent lock closure. Via software TwinComm USB the options 'Manual closing with code query' and 'Automatic closing with door switch' have not been selected.

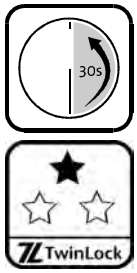
1. Press key `Enter` and release it immediately.
   The system checks its status. Date and time are on display.

2. With key < or key > select `Close` and press key `Enter`.
   `Close` *and, as the case may be,* `Lock 1` *are on display. If the lock is closed, menu* `Close` *cannot be selected.*

3. With key < or key > select the lock, if necessary, and press `Enter`.
   `Close | Please wait` *is on display. The lock bolt engages.*
   `Close | Lock closed no.` *is on display.*

You have successfully closed a lock.

3.9.11 Closing a Lock with Code Input



In order to close a lock by entering code, either PIN- or Fingerprint code or card code (TwinCard code access) is sufficient.

Settings Via software TwinComm USB, the option 'Manual closing with code query' has been selected.
Boxes **Release, Close & code**, **PIN code** or **Fingerprint** or **Card** have been ticked (AE: checked) for you.

1. Press key `Enter` and release it immediately.
   The system checks its status. Date and time are on display.

2. With key < or key > select `Close` and press key `Enter`.
   `Close` *and, with a system with 2 or 3 locks,* `Lock 1` *are on display.*

3. If necessary, select the lock with < or > and press `Enter` again.
   `Code entry | User: Master` *is on display.*

4. With < and > and `Enter` select your user number.
   `User No | PIN code` is on display.

5. Select `PIN-Code` or `Code card` or `Fingerprint` and enter code or insert card.
   See the instructions 'Open a Lock by ...' at the beginning of this chapter. `Close | Please wait` is on display. The lock bolt engages.
   `Close | Lock closed no.` is on display.

You have successfully closed a lock.

3.9.12 Closing a Lock Automatically with the Door Switch

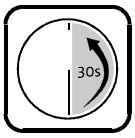
This option can be set via optional software TwinComm USB.

Settings TwinXT or TwinAlarm are connected and activated. On tab 'Settings' of TwinComm USB, the option 'Automatic closing with door switch' is selected. The bolt work switch is not in a position in which it prevents automatic closing.

- Close the door of the safe / box / container.
  Via regular checks on the state of door- and bolt system switches the system registers that the door has been closed and the system closes the locks automatically.

The lock has closed automatically.

3.9.13 Setting / Arming a Burglar Alarm System (BAS)



Depending on the setting in TwinComm USB ('Settings / TwinAlarm / Arming with code' on / off), operators either enter PIN code / insert their code card in order to arm the BAS or they do not have to do so.

Settings TwinAlarm and BAS are connected, TwinAlarm is activated, BAS is disarmed and all locks are closed. Only under these conditions, menu `Arming BAS` for arming the BAS is on display.
In menu `Settings` `Alarm devices` the system manager has set `TwinAlarm` to `* yes`. For you, he has, if necessary, selected options **Release**, **PIN code** and / or **Card** and / or **Fingerprint** of the user matrix.

1. Lock the system by closing lock 1 or, if necessary, all locks.
   See 'The System Status' in this chapter. The system is locked.

2. Press key `Enter` and release it immediately.
   The system checks its status. Date and time are on display.

3. With key < or key > select `Arming BAS` and afterwards press `Enter`.
   In case `! BAS armed !` is on display, you already have armed the BAS successfully.

With option 'Arming with code' set, `Code entry | User: Master` *and* `PIN code` *are on display.*

- Select your user number with key < and key > and `Enter` and confirm `PIN code` or with < or > select `Code card` or `Fingerprint` and `Enter` and open lock 1.

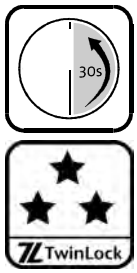
Depending on your selection, the appropriate menus are displayed. The procedures of code entry and card insertion are the same as for opening a lock. See the instructions for lock opening at the beginning of this chapter.

`User: No. | Please wait` *is on display. An acoustic signal beeps.* `User: No. | ! BAS armed !` *is on display.*

You have successfully armed (set) the burglar alarm system.

3.10 Programming System Settings

3.10.1 Setting the Date and the Time of Day



All time-based functions and the correctness of the protocol depend on the proper setting of date and time. Clock change (Daylight Saving Time) in spring and autumn will be automatic if this option is activated on tab 'Settings' of TwinComm USB (default setting).

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.

2. With menu key < or menu key > select `Settings` and press key `Enter`.
   `Settings | Master code` *is on display.*

3. With key < or key > select `Date / Time` and press `Enter`.
   `System manager | Code entry, 0123456789` *and* `Code:` *are on display.*

4. With < or > select a number of the system manager code and press `Enter`. In this way enter all numbers of the code.
   The cursor flashes at the first digit of the time currently set. If you press the `Clear` *key twice, the system will keep its time setting.*

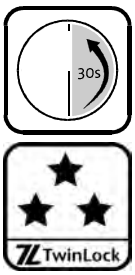
5. With < and > and `Enter` set the current time.
   The cursor '>' flashes next to the day of the week (Mo/Tu/We/Th/Fr/Sa/Su).

6. With < or > select the two first letters of the current day of the week and press `Enter`.
   The first digit of the date flashes.

7. Enter day, month and year in the same way as you entered the time.
   `Date / Time | Saved` *are on display.*

You have set time and date successfully.

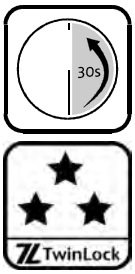
3.10.2 Switching On / Off TwinXT or TwinAlarm



1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.
2. With key < or key > select `Settings` and press key `Enter`.
   `Settings | Master code` *is on display.*
3. With menu key < or > `Alarm devices` and press `Enter`.
   `System manager | Code entry`, `0123456789`, *as the case may be, and* `Code:` *are on display. See paragraph 'Entering PIN Code'.*
4. With < or > select a number of the system manager code and press `Enter`. In this way, enter all numbers of the code.
   `Alarm devices | TwinXT` *is on display.*
5. Confirm `TwinXT` by pressing `Enter` or with < or > select `TwinAlarm` or `TwinIP` and confirm with `Enter`.
   `Enable`, *the device selected, and* `*=yes *=no` *are on display.*
6. To activate a device, with < or > select `*=yes` and press `Enter`, in order to deactivate a device, select `*=no` and press `Enter`.
   `Enable`, *the selected device,* `Deleted` *or* `Saved` *are on display.*

You have successfully switched on / off TwinAlarm / TwinXT / TwinIP.

3.10.3 Setting the CIT Function (2 Groups of Users)



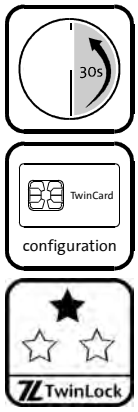
Also see 'Operation with CIT Function Selected' in this chapter.

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.
2. With menu key < or > select `Settings` and press key `Enter`.
   `Settings | Master code` *is on display.*
3. With menu key < or > select `CIT function` and press `Enter`.
   `System manager | Code entry`, `0123456789`, *as the case may be, and* `Code:` *are on display. See paragraph 'Entering PIN Code'.*
4. With < or > select a number of the system manager code and press `Enter`. In this way, enter all numbers of the code.
   `CIT function |*=yes *=no` *is on display.*
5. With menu key < or > select
   - `*=yes` in order to activate the device /
   - `*=no` in order to deactivate it and press `Enter`.

   `CIT function | Deleted` *or*
   `CIT function | Saved` *are on display.*

You have successfully activated / deactivated the CIT function.

3.10.4 Exporting the Protocol (TwinComm USB)



Settings Boxes **Release**, **Service**, **PIN code** and / or **Card** of the user matrix have been ticked (AE: checked) for you.

Take the optional PC software TwinComm USB and optional TwinCard configuration II.

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.

2. With key < or key > select `Import / Export` and press key `Enter`.
   `Import / Export | Configuration` is on display.

3. With key < or > select `Protocol` and press `Enter`.
   `Code entry | User: Manager` is on display.

4. Confirm with `Enter` or with key < or key > and with `Enter` select `Master` or select your user number.
   `System manager`, `Master` or `User no.` and `PIN code` are on display. Entering one kind of code is sufficient.

5. Confirm with `Enter` and enter PIN code or with < or > select `Code card` or `Fingerprint`.
   See the instructions for opening locks at the beginning of the chapter.
   `Please wait` and afterwards
   `Export log | Insert card` are on display.

6. Insert TwinCard configuration II into the operation unit.
   See 'Inserting a Chip Card into the Operating Unit'.
   `Export log | >>>` is on display. Data are transferred to the card. The number of brackets indicates the progress.
   `Export log | Remove card` is on display.

7. Remove the card from the operating unit.
   `OK` and afterwards `Import / Export` are on display.

You have successfully transferred the protocol onto a chip card.

3.10.5 Displaying / Printing the Protocol (TwinComm USB)

Opening – and closing processes, code input, configuration tasks and attempts of a manipulative nature are logged.

Settings Protocol data have been saved on chip card.

Take the optional software TwinComm USB and the optional chip card TwinCard configuration II.

1. Start program TwinComm USB at your computer and select button `Protocol`.
   The tab 'Protocol' is displayed at the screen.

2. Insert card TwinCard configuration II with the chip on top into the reader.

3. In window TwinComm USB select the button `Read chip card`.
   Protocol data are displayed on the screen.

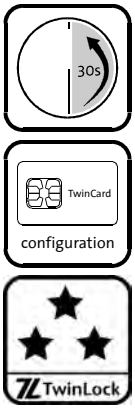
4. Optional: Select button `Update user` in case user data have been modified since last loading the card. .
   New user data are on display in the protocol.

5. Optional: Select the button with the printer icon in order to print the protocol.
   The protocol is printed. With button `Save log file` you can export it as CSV file into program Excel.

6. Remove the chip card from the card reader.

You have successfully displayed and printed the protocol.

3.10.6 Importing the Configuration



Settings With TwinComm USB, a valid configuration has been programmed (and saved).

Take the optional software TwinComm USB and the optional TwinCard configuration II.

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.

2. With < or > select `Import / Export` and press `Enter`.
   `Import / Export | Configuration` is on display.

3. Confirm with `Enter`.
   `Import / Export | Import` is on display.

4. Confirm with `Enter`.
   `System manager | Code entry`
   and afterwards `Code:` are on display. See paragraph 'Entering PIN Code'.

5. With < or > select a number of the system manager code and press `Enter`. In this way, enter all numbers of the code.
   `Please wait` and `Data import | Insert card` are on display.

6. Insert chip card TwinCard configuration II into the operating unit.
   See 'Insert Chip Card into Operating Unit'.
   `1 >>> 5` is on display. The Configuration is imported from the card. If the configuration contains incorrect parameters, error messages will be displayed. See the following list.
   `5 >>> 5` and `Data import | Remove card` are on display.

7. Remove the chip card from the operating unit.

You have configured the system successfully.

3.10.7 Configuration Import: Error Messages

During the import of a configuration, the error messages listed below may be on the display of the operating unit, which features two lines.

- Modify invalid parameters via optional software TwinComm USB and import the configuration again.

Messages in the first line of the display:

`Config. error` in the first line indicates that an invalid value has been allotted to a parameter.

`Lock system` in the first line indicates that the configuration does not fit to (the hardware of) the system.

Messages in the second line of the display:

`Alarm delay`

! The alarm delay triggered simultaneously with silent alarm has been set to last longer than the permitted 0-99 minutes.

✓ *Enter a value within the permitted range of values.*

`Block period`

! At least one invalid date has been entered for 'Block(ed) period'.

✓ *Amend the data for timer program 'Blocked period'.*

`CIT user`

! The user number of the first 'CIT user' is not within the permitted range of '01-99'.

✓ *Enter a value within the permitted range of values.*

`Close&Code`

! 'Manual closing with code query' and 'Automatic Closing with door switch' / 'Opening lock 1 -> 2' are activated (on tabs 'Settings / -1').

✓ *Tick off (AE: check off) one of the options (TwinComm USB).*

`Door open`

! The value for 'Open door monitoring' is not within the permitted range of '00-99 minutes'.

✓ *Enter a value within the permitted range of values.*

`Image quality`

! The value 'Image quality' is not within the permitted range of '20-99'.

✓ *Enter a value within the permitted range of values.*

`Min. Minutiae`

! The lower limit for 'Min. Minutiae' is not within the permitted range of '09-50'.

✓ *Enter a value within the permitted range of values.*

`Old code`

! The value for 'Code validity' is not within the permitted range of 0-99 months.

✓ *Enter a value within the permitted range of values.*

`Open`

! The value for parameter 'Opening lock 1 -> 2' is not within the permitted range of 00-99 minutes.

✓ *Enter a value within the permitted range of values.*

`Parallel code`

! 'Parallel code' and 'Dual code / 4-eyes (Opening)' are ticked.

✓ *Tick off one of the options (Tab 'Settings', TwinComm USB).*

`Part locked time`

! At least one invalid time specification has been entered for 'Part lock(ed) time'.

✓ *Amend the data for timer program 'Part lock time'.*

`PIN code`

! Too few PIN codes are registered in the system. If the configuration were imported, no one could open the lock.

✓ *Increase the number of authorised users in the system.*

`Security level`

! The minimum requirement value for 'Security level' is not within the permitted range of '30-99'.

✓ *Enter a value within the permitted range of values.*

`Silent alarm`

! The value for 'Alarm digit' is not within the permitted range of '01-09'.

✓ *Enter a value within the permitted range of values.*

`Special days`

! An invalid date has been entered for at least one 'Special day'.

✓ *Amend the data for timer program 'Special days'.*

`Temperature`

! The value for 'Sensor temperature' is not within the permitted range of '00' or '18-50 ° C'.

✓ *Enter a value within the permitted range of values*

`Time delay`

! The value for 'Unlocking delay' / 'Time delay' of the lock is not within the permitted range of '00-99 minutes'.

✓ *Enter a value within the permitted range of values*

`TwinAlarm`

! TwinXT as well as TwinAlarm are activated both.

✓ *Deactivate the device not part of the system.*

`Weekly program`

! An invalid date has been entered for 'Weekly program'.

✓ *Enter a value within the permitted range of values.*

3.10.8 Exporting the Configuration (TwinComm USB)

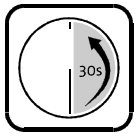
You can export the configuration of the lock system via chip card to the optional software TwinComm USB, in order to save it, for example.

Take the optional software TwinComm USB and the optional chip card TwinCard configuration II.

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.
2. With menu key < or > select `Import / Export` and press key `Enter`.
   `Import / Export | Configuration` *is on display.*
3. Confirm with `Enter`.
   `Import / Export | Import` *is on display.*
4. With < or > select `Export` and press `Enter`.
   `System manager | Code entry`, `0123456789` *and* `Code:` *are on display.*
5. With < or > select a number of the system manager code and press `Enter`. In this way enter all numbers of the code.
   `Please wait` *and* `Data export | Insert card` *are on display.*
6. Insert the chip card TwinCard configuration II into the operation unit.
   See 'Inserting Chip Card into Operating Unit'.
   `>>>` *is on display. The number of brackets increases as the data are transferred. Configuration data are written onto the chip card.*
   `Data export | Remove card` *is on display.*
7. Remove the chip card from the operating unit.

You have successfully transferred the configuration onto a chip card.

3.10.9 Selecting a Language



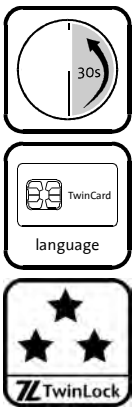
You can choose one of three languages stored in the operating unit before. Also see 'Importing a Language' below.

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.
2. With key < or key > select `Import / Export` and press key `Enter`.
   `Import / Export | Configuration` *is on display.*
3. With < or > select `Language` and confirm with `Enter`.
   `Language | 1 Deutsch` *is on display. You can choose between languages no. 1, 2 or 3. The language you select is named* `Selected language` *in the following text.*

4. Select the language with < / > and confirm with `Enter`.
   `Selected language | Saved` and afterwards `Selected language | OK` are on display.

You have changed the language of the display at the operating unit successfully.

3.10.10 Importing a Language



In the operating unit, three interchangeable languages can be saved.

Take the optional chip card TwinCard language.

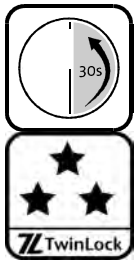
1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.
2. With menu key < or > select `Import / Export` and press key `Enter`.
   `Import / Export | Configuration` is on display.
3. With < or > select `Language` and confirm with `Enter`.
   `Language | 1 Deutsch` is on display.
4. With < or > select `Data import` and `Enter`.
   `Language | Data import`, `System manager | Code entry`, `0123456789` and `Code:` are on display.
5. With < or > select a number of the system manager code and press `Enter`. In this way, enter all the numbers of the code.
   `Language |Please wait` and `Language | Language no.: 1<` are on display. The cursor flashes.
6. With < or > select the number of the new language and press `Enter`.
   The language assigned to that number before will be deleted. `Import language | Insert card` is on display.
7. Insert chip card TwinCard language into the operating unit.
   See 'Inserting a Chip Card into the Operating Unit'. `Data import | Language` and `>>>` are on display. The number of brackets increases during data transfer. `Data import | Remove card` is on display.
8. Remove the chip card from the operating unit.

You have successfully imported the language.

3.11 Administrating Users

3.11.1 Changing the System Manager Code

With the system manager code (manager code of lock 1) you cannot open the lock but configure the system.



Caution

With the system manager code in ex works version, your system is not protected.
Change ex works code as soon as possible. Never use series of numbers corresponding with personal data.

Caution

Without system manager code, you cannot configure the system.
Save the system manager code in a secure place accessible to the system manager only.

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.

2. With key < or key > select `Settings` and press key `Enter`.
   `Settings | Master code` *is on display.*

3. With < or > select `Manager code` and `Enter`.
   `Code entry | Lock 1<` *is on display.*

4. With 2 or 3 locks in the system, with key < or > and `Enter` select lock 1.
   `Code entry`, `System manager`, `0123456789` *and* `Code:` *are on display.*

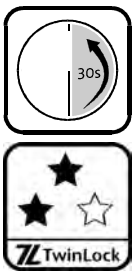
5. With < or > select a number of the system manager code and press `Enter`. In this way, enter all the numbers of the code.
   `System manager | Please wait`, *and*
   `New manager code | Code:` *are on display.*

6. Enter the new system manager code.
   `Confirm code | Code:` *is on display.*

7. Repeat entering the new system manager code.
   `New manager code | Please wait` *and*
   `New manager code | Saved` *are on display.*

You have changed the system manager code successfully.

3.11.2 Changing the Master Code / CIT Master Code



With the master - and, as it may be, the CIT master code of the lock you can administrate users and, optionally, open the lock.

Caution

With the master code in ex works version, your system is not protected.
Change ex works code as soon as possible. Never use series of numbers corresponding with personal data.

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.

2. With menu key < or > select `Settings` and press key `Enter`.
   `Settings | Master code` *is on display.*

3. Confirm `Master code` with `Enter`.
   `Code entry` *and, as it may be,* `Lock 1<` *is on display.*

4. With menu key < or > select the lock, if necessary, and press `Enter`.
   `Code entry`, `Master`, `0123456789`, *as the case may be, and* `Code:` *are on display. Also see paragraph 'Entering PIN Code' above.*
   With the CIT function set, `Code entry` *and* `User: Master` *are on display. With < or > you can select* `CIT master`*. In all other respects this instruction for changing the master code also applies to the CIT master code.*

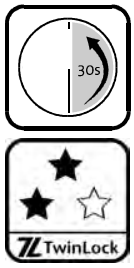
5. With < or > select a number of the 'old' master - / CIT master code and press `Enter`. In this way, enter all the numbers of the code.
   `Master | Please wait`, *and*
   `New master code | Code:` *are on display.*

6. Enter the new master - / CIT master code.
   `Confirm code`, `0123456789` *and* `Code:` *are on display.*

7. Repeat entering the new master - / CIT master code.
   `New master code | Please wait` *and*
   `New master code | Saved` *are on display.*

You have changed the master – or the CIT master code successfully.

3.11.3 Registering PIN Code for Users / Operators



The bearer of the master code (lock master) and the CIT master, as it may be, can register PIN code for users at the lock. In order to be able to open with PIN code, users must be authorised to do so in user matrix of TwinComm USB.

	Caution
	With Comfort Systems: If PIN codes are registered at lock 1 before TwinAlarm is installed and activated, the PIN codes will not be saved in TwinAlarm. These users (operators) cannot disarm the burglar alarm system with these PIN codes. Make sure TwinAlarm is installed and activated before you register PIN codes for users at lock 1.
Settings	If a burglar alarm system is part of the system install and activate TwinAlarm before registering PIN codes.

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.

2. With key < or > select `Settings` and press `Enter`.
   `Settings | Master code` *is on display.*

3. With < or > select `PIN code` and press `Enter`.
   `PIN-Code | Register` *is on display.*

4. With < or > select `Register` and press `Enter`.
   `Register | Change code` *is on display.*

5. With < or > select `New user` and press `Enter`.
   `Code entry` *and, as it may be* `Lock 1` *is on display.*

6. With < or > select the lock, if necessary, and press `Enter`.
   With the CIT function set, `Code entry` *and* `User: Master` *are on display. With < or > you can select* `CIT master` *and press* `Enter`.
   Without the CIT function set, `Code entry`, `Master`, `0123456789` *and* `Code:` *are on display.*

7. With < or > select a number of the master - / CIT master code and press `Enter`. In this way, enter all the numbers of the code.
   `Master code` *or* `CIT code`, `Please wait` *and afterwards* `Register | User: 01` *are on display.*

8. With < or > and `Enter` select the user for whom to register PIN code.
   `New user code | Code:` *is on display.*

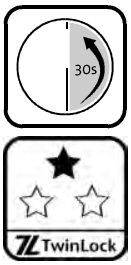
9. Enter the new user PIN code.
   `Confirm code | Code:` *is on display.*

10. Repeat entering the new PIN code.
    `PIN code | Please wait` *and* `User No. | Saved` *and afterwards* `Another code? | *= yes *=no` *are on display. You can register PIN code for further users.*

11. In order to register further PIN code, simply select `*= yes` and repeat steps 8 - 11 for other users.
    Select `*= no` in order to end registering code.

You have successfully registered PIN code for users.

3.11.4 Changing a PIN Code



Operators can change their PIN code when the system is unlocked.

Settings At least boxes **PIN code**, **Open locks** and **Release** have been ticked (AE: checked) for you in the user matrix. The lock master has registered your PIN code at the lock.

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.

2. With key < or > select `Settings` and press `Enter`.
   `Settings | Master code` *is on display.*

3. With < or > select `PIN code` and press `Enter`.
   `PIN code | Register` *is on display.*

4. With < or > select `Register` and press `Enter`.
   `Register | Change code` *is on display.*

5. Confirm `Change code` with `Enter`.
   `Old Code` *and* `Lock 1`*, as may be the case, are on display.*

6. With < or > select the lock, if necessary, and press `Enter`.
   `Old Code | User: 01` *is on display.*

7. With < or > and key `Enter` select your user number.
   `User no.`, `0123456789` *and* `Code:` *are on display. Also, see paragraph 'Enter PIN-Code' above.*

8. With < or > select a number of your registered PIN code and press `Enter`. In this way, enter all the numbers of the code.
   `New user code` `0123456789` *and* `Code:` *are on display.*

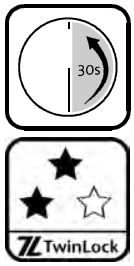
9. Enter your new PIN code.
   `Confirm code` *... and* `Code:` *are on display.*

10. Repeat entering your new PIN code. .
    `PIN code | Please wait` *and*
    `User no. | Saved` *are on display.*

You have changed your PIN code successfully.

3.11.5 Deregistering PIN Code

Caution



Danger of a configuration error:
Opening the lock might become impossible.
A lock, at which too few codes are registered, cannot be opened. Especially in case you have selected the option 'Dual code', make sure that at least as many codes as required are authorised and registered.

1. Select menu `Settings | PIN code`.
   For an exact instruction for this step see paragraph above, 'Changing PIN Code', steps 1-3. `PIN code | Register` *is on display.*

2. With key < or > select `Deregister` and key `Enter`.
   `Code entry` *and* `Lock 1`*, as the case may be, are on display.*

3. With key < or > select the lock, if necessary, and press `Enter`.
   With the CIT function set, `Code entry` *and* `User: Master` *are on display. With < or > you can select* `CIT master` *and press* `Enter`.

   Without the CIT function set, `Code entry`*,* `Master`*,* `0123456789` *and* `Code:` *are on display. Also see paragraph 'Entering PIN Code' above.*

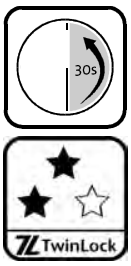
4. Enter the master - / CIT master code.
   `Master code` *or* `CIT code`*,* `Please wait` *and afterwards* `Deregister | User: 01` *are on display.*

5. With < or > and key `Enter` select the user number to be deregistered.
   `PIN code | Please wait` *and*
   `User no. | Deregistered` *and afterwards*
   `Another code? | *= yes *=no` *are on display.*
   You can continue deregistering code for users.

6. Simply select `*= yes` and repeat step 5 for other users.
   Select `*= no` to end deregistering users.

You have successfully deregistered PIN code.

3.11.6 PIN Code User Display



The lock master and the CIT master, as the case may be, can display for which users PIN code is registered. With the CIT function selected, lock master as well as CIT master can display the PIN code users of their user group only.

1. Select menu `Settings | PIN code`.
   For an exact instruction for this step, see paragraph above, 'Changing PIN Code', steps 1-3. `PIN code | Register` is on display.

2. With key < or > select `User display` and press `Enter`.
   `Code entry` and `Lock 1`, as the case may be, are on display.

3. With key < or > select the lock, if necessary, and press `Enter`.
   With the CIT function set, `Code entry` and `User: Master` are on display. With < or > you can select `CIT master` and press `Enter`.

   Without the CIT function set, `Code entry`, `Master`, `0123456789` and `Code:` are on display. Also see paragraph 'Entering PIN Code' above.

4. With < or > select a number of the master - / CIT master code and press `Enter`. In this way, enter all the numbers of the code.
   `Please wait` and afterwards
   `PIN users: No.| User code No.:(N)OK` are on display. The total number of registered PIN code users is on display in the first line. In the second line a user number and next to it, `OK` / `NOK` is displayed.

5. With < and > browse through PIN code settings for user numbers.
   The letters OK and NOK inform about the state:
   `NOK` = no PIN code registered for user number displayed.
   `OK` = there is PIN code registered for user number displayed.

You have successfully displayed how many and which users have PIN code registered for them.

3.11.7 Registering a Code Card

The lock master and the CIT master, as it may be, can register code cards TwinCard code access for themselves and for users.

Take a chip card TwinCard code access per user.

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.

2. With key < or > select `Settings` and press `Enter`.
   `Settings | Master code` *is on display.*

3. With < or > select `Code card` and press `Enter`.
   `Code card | Register` *is on display.*

4. Confirm with `Enter`.
   `Code entry` *and* `Lock 1`*, as the case may be, are on display.*

5. With key < or > select the lock, if necessary, and press `Enter`.
   With the CIT function set, `Code entry` *and* `User: Master` *are on display. With < or > you can select* `CIT master` *and press* `Enter`.

   Without the CIT function set, `Code entry`*,* `Master`*,* `0123456789` *and* `Code:` *are on display.*

6. With < or > select a number of the master - / CIT master code and press `Enter`. In this way, enter all the numbers of the code.
   `Master code`*, or* `CIT code`*,* `Please wait` *and afterwards* `Register | User: 01` *are on display.*

7. With < or > and key `Enter` select the user number for which a card is to be registered.
   `User: No. | Insert card` *is on display.*

8. Insert the chip card TwinCard code access into the operation unit (see paragraph 'Inserting a Chip Card into the Operating Unit' above).
   `Please wait` *and afterwards* `Remove card` *are on display.*

9. Remove the card.
   `User no. | Registered` *and afterwards* `Another code? | *= yes *=no` *are on display.*
   You can continue registering code cards for users.

10. In order to register another card select `*= yes` and repeat steps 7-10.
    Select `*= no` to end registering cards.

You have successfully registered code cards.

3.11.8 Deregistering a Code Card

The lock master and the CIT master, as the case may be, can deregister code cards TwinCard code access. Even users authorised to open with code card cannot open the lock with a deregistered card.

Caution

Danger of a configuration error: Unintentionally, opening the locks can be made impossible.
A lock at which too few codes are registered cannot be opened. Especially in case you have selected options 'Dual code' or 'Forced sequence', make sure that at least as many codes as required are authorised and registered.

1. Select menu `Settings | Code card`.
   For exact instructions for this step see paragraph 'Registering a Code Card', steps 1-3. `Code card | Register` *is on display.*

2. With < or > select `Deregister` and press `Enter`.
   `Code entry` *and* `Lock 1`*, as the case may be, are on display.*

3. With key < or > select the lock, if necessary, and press `Enter`.
   With the CIT function set, `Code entry` *and* `User: Master` *are on display. With < or > you can select* `CIT master` *and press* `Enter`.

   Without the CIT function set, `Code entry`*,* `Master`*,* `0123456789` *and* `Code:` *are on display. Also see paragraph 'Entering PIN Code' above.*

4. Enter the master - / CIT master code.
   `Master code`*, or* `CIT code`*,* `Please wait` *and afterwards* `Deregister | User: 01` *are on display.*

5. With < or > and key `Enter` select the user number for which a card is to be deregistered.
   `User no. | Please wait`*,*
   `User no. | Deregistered` *and afterwards*
   `Another code? | *= yes *=no` *are on display.*
   You can continue deregistering code cards for users.

6. In order to deregister further cards, select `*=yes`,
   and repeat steps 5 and 6 for other users.
   Select `*=no` in order to stop deregistering code cards.

You have successfully deregistered code cards.

3.11.9 Code Card User Display

The lock master and the CIT master, as the case may be, can display for which users code cards are registered at a lock. With the CIT function selected, lock - as well as CIT master can see the card users of their user group only.

1. Select menu `Settings | Code card`.
   For exact instructions for this step, see paragraph 'Registering a Code Card', steps 1-3. `Code card | Register` *is on display.*

2. With < or > select `User display` and press `Enter`.
   `User display` *and* `Lock 1`*, as the case may be, are on display.*

3. With key < or > select the lock, if necessary, and press `Enter`.
   With the CIT function set, `Code entry` *and* `User: Master` *are on display. With < or > you can select* `CIT master` *and press* `Enter`.
   Without the CIT function set, `Code entry`*,* `Master`*,* `0123456789` *and* `Code:` *are on display. See paragraph 'Entering PIN Code' above.*

4. With < or > select a number of the master - / CIT master code and press `Enter`. In this way, enter all the numbers of the code.
   `Please wait` *and afterwards*
   `Cards: No.| Card: No.: NOK/OK` *are on display.*
   The total number of registered code cards is on display in the first line.
   In the second line, a user number and next to it `OK` */* `NOK` *is displayed.*

5. With < and > browse through code card settings for user numbers.
   The letters OK and NOK inform about the state:
   `NOK` *= no code card registered for the user number displayed.*
   `OK` *= there is a code card registered for the user number displayed.*

You have successfully displayed for which users code cards are registered.

3.11.10 Fingerprint: Survey

By entering fingerprint code alone, users cannot open locks. Users additionally also have to enter PIN code and / or insert a code card before a lock opens.

In order to enable users to enter fingerprint code, the system manager has to authorise them via user matrix of TwinComm USB. Also see 'Authorising the Users' in this chapter.

In order to be able to enter fingerprint code, every user also has to have fingerprint code registered at a lock. Only the master of a lock and the CIT master, as the case may be, can register user fingerprint at the lock with the users providing their biometric data.

Fig. 22: Operating unit with guiding for fingers

Users can practice scanning with menu `Scan test` (see the following instruction 'Fingerprint: Scan Test') and find out which fingerprint data values are typical for them.

These values are

- the number of minutiae (individually distinctive features)
- the typical 'image quality' of a finger print
- the extent of congruence ('matching') of the data extracted during the repeated scanning procedures.

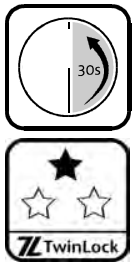
Once these values have been established, the lock master can determine the minimal number of minutiae, the lower limit for image quality and the security level for users individually. General lower limits for these parameters are set (and can be adjusted) via software TwinComm USB.

After that, the lock master together with the users can register fingerprint code. See instruction 'Registering Fingerprint Code' in this chapter.

Also see the instructions 'Fingerprint: Determining Min. Minutiae', 'Fingerprint: Image Quality' and 'Fingerprint: Security Level' in this chapter.

The system manager can adjust the sensor temperature.

3.11.11 Fingerprint: Scan Test



With menu `Scan test` you can practice scanning and find out about biometrical data characteristical for you. After that, your individual settings for fingerprint can be programmed. Also see the other instructions concerning fingerprint in this chapter.

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.

2. With key < or key > select `Settings` and press `Enter`.
   `Settings | Master code` *is on display.*

3. With < or > select `Fingerprint` and press key `Enter`.
   `Fingerprint | Scan test` *is on display.*

4. Confirm with key `Enter`.
   `Scan Test | <<SCAN>>` *is on display. As long as the brackets around* `<<SCAN>>` *are animated, the fingerprint sensor is activated.*

5. Put a finger inside the guiding (fingertip pointing upwards and touching the curve on top) and steadily move it downwards.
   `Minu:XX Quali:XX | OK` *will be on display if the image quality as at least as good as required. 'Minu' is short for 'Minutiae', 'Quali' for image quality.*

   `Minu:XX Quali:XX | Not identified!` *would be on display if one of the two values did not meet the requirements.*

6. Select the same finger and collect further data.

   `Matching: No.` *is on display after a finger has been scanned a second time. The number displayed indicates the degree of congruence of the data extracted during the rounds. Based on this value for 'Matching' the 'Security level' for a user can be determined During one scan test, a finger can be scanned three times.*

7. When `Fingerprint | Scan Test` is displayed, confirm with key `Enter` in order to scan another finger.
   `Scan Test | <<SCAN>>` *is on display again.*
   `Scan test | Bad image` *would be on display if the quality were not to meet the requirements.*
   `Scan test | No image` *would be on display if the sensor were not to recognise the presence of a finger.*

You have successfully practiced scanning and found out about typical features of one of your fingerprints.

3.11.12 Fingerprint: Determining Min. Minutiae

The lock master can decide about the minimal number of minutiae (distinguishing marks, value range '9 – 50', preset value '18') for fingerprint code of a user.

Value range: 09 – 50, preset value: 18, lower limit: 9.

After that, the lock master together with the user registers the user's fingerprint code. See 'Registering Fingerprint Code' in this chapter.

Settings With menu `Scan test` (see instruction 'Fingerprint: Scan Test' above) the users have learned about the number of minutiae typical for the fingers they use.

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.

2. With key < or key > select `Service` and press `Enter`.
   `Service | Reset` *is on display.*

3. With < or > select `Fingerprint` and press key `Enter`.
   `Service | Fingerprint` *is on display.*

4. Press `Enter` again.
   `Fingerprint | Status / Info` *is on display.*

5. With < or > select `Min.Minutiae` and press key `Enter`.
   `Code entry` *and* `Lock 1`*, as the case may be, are on display.*

6. Confirm with `Enter` or, if necessary, select lock 2 or 3.
   With the CIT function selected, `Code entry | User: Master` *is on display. With < or > you can select CIT master and press* `Enter`*.*
   Without the CIT function selected, `Code entry`*,* `Master`*,* `0123456789` *and* `Code:` *are on display.*

7. Select the digits of the (CIT) master code with < and > and `Enter`.
   `(CIT) Master | Please wait` *and afterwards* `Min.Minutiae | User: (CIT) Master` *are on display.*

8. With < and > and `Enter` select the user number.
   `Min.Minutiae | 18` *is on display, for example.*
   As the lower limit set the value you have found out with menu `Scan test` *minus a small tolerance (approx. 1-2). With the optional software TwinComm USB, you can increase the general lower limit ('9' ex works).*

9. Increase or decrease the value with < or > and `Enter`.
   `Min.Minutiae | Saved` *is on display.*

You have successfully specified the lower limit of minutiae required in a fingerprint code of a specific user.

3.11.13 Fingerprint: Image Quality

The parameter 'Image quality' is used to make sure only fingerprint images of a good quality with unique distinguishing marks are accepted. A value of 60 indicates very good quality. It is almost impossible to achieve results with higher values.

Range of values: 20 – 99, default value: 40, lower limit 20

Possible causes for bad image quality:

Finger moved too fast / too slow over sensor, pressure of finger on sensor too low / too high, finger too dry / too moist, minor injuries

Settings Users are authorised for fingerprint (see paragraph 'Authorise the Users'). With menu `Scan test` (see instruction 'Fingerprint: Scan Test' above) the users have learned about the 'image quality' typical for the fingers they use.

After every round of Scan Test, the value for image quality is displayed. We recommend setting the lower limit for 'image quality' individually to approx. 90% of the value displayed for users when they test scanning.

1. Select menu `Service | Fingerprint`.
   For a detailed instruction see paragraph 'Fingerprint: Determining Min. Minutiae', steps 1-4.
   `Fingerprint | Status / Info` is on display.

2. With < or > select `Image quality` and press `Enter`.
   `Code entry` and `Lock 1`, as the case may be, are on display.

3. Press key `Enter` or, if necessary, select lock 2 or 3.
   With the CIT function selected, `Code entry | User: Master` is on display. With < or > you can select CIT master and press `Enter`.
   Without the CIT function selected, `Code entry`, `Master`, `0123456789` and `Code:` are on display.

4. Select the digits of the (CIT) master code with < and > and `Enter`.
   `(CIT) Master | Please wait` and afterwards
   `Image quality | User: (CIT) Master` are on display.

5. With < and > and `Enter` select the user number.
   `Image quality | XX` is on display.

6. Increase or decrease the value with < or > and `Enter`.
   `Image quality | Saved` is on display.

   The message `Bad image` would be on display if a lock master and a user tried to register fingerprint code with fewer minutiae.

You have successfully specified the lower limit for 'Image quality' for fingerprint code of a user individually.

3.11.14 Fingerprint: Security Level

The Security level indicates the extent of similarity ('Matching') which a scanned fingerprint must have in common with fingerprint data saved in order to be found identical. So this parameter determines whether a person is identified or not. This parameter has direct impact on the security of the system.

Range of values: 30 – 99, default value: 60, lower limit 30.

Setting Users are authorised for fingerprint (see paragraph 'Authorise the Users'). With menu `Scan test` (see 'Fingerprint: Scan Test' above) the users have learned about the value for 'Matching' that is typical for the fingers they scan.

After two rounds of `Scan test`, the value for 'Matching' is displayed. We recommend to subtract about 10-15 from that value and define the result as 'Security level' for the user.

1. Select menu `Service | Fingerprint`.
   For a detailed instruction see paragraph 'Fingerprint: Determining Min. Minutiae', steps 1-4.
   `Fingerprint | Status / Info` is on display.

2. With < or > select `Security level` and press key `Enter`.
   `Code entry` and `Lock 1`, as the case may be, are on display.

3. Press key `Enter` or, if necessary, select lock 2 or 3.
   With the CIT function selected, `Code entry | User: Master` is on display. With < or > you can select CIT master and press `Enter`.
   Without the CIT function selected, `Code entry`, `Master`, `0123456789` and `Code:` are on display.

4. Select the digits of the (CIT) master code with < and > and `Enter`.
   `(CIT) Master | Please wait` and afterwards
   `Security level | User: (CIT) Master` are on display.

5. With < or > select the user number and press `Enter`.
   `Security level | XX` is on display.

6. Increase or decrease the value with < or > and `Enter`.
   `Security level | Saved` is on display.

You have successfully specified the lower limit for 'Security level' for fingerprint code of a user individually.

3.11.15 Registering Fingerprint Code

The lock master can register fingerprint code for a user together with the user. Three successful scanning processes within one sitting are required in order to register fingerprint code.

One of the fingers can be declared 'Alarm finger' with which silent alarm is triggered during lock opening.

Settings Users are authorised for fingerprint (see paragraph 'Authorise the Users'). Via menu `Scan test` the user has learned about the characteristics of his fingerprint data and the lock master has set the parameters `Min.Minutiae`, `Image quality` and `Security level` individually for the user.

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.

2. With key < or key > select `Settings` and press `Enter`.
   `Settings | Master code` is on display.

3. With < or > select `Fingerprint` and press key `Enter`.
   `Fingerprint | Scan Test` is on display.

4. With < or > select `Register` and `Enter`.
   `Code entry` and `Lock 1`, as the case may be, are on display.

5. Confirm with key `Enter` or, if necessary, select lock 2 or 3.
   With the CIT function selected, `Code entry | User: Master` is on display. With < or > you can select CIT master and select `Enter`.
   Without the CIT function selected, `Code entry`, `Master`, `0123456789` and `Code:` are on display.

6. Select the digits of the (CIT) master code with < and > and `Enter`.
   `(CIT) Master | Please wait` and afterwards `Fingerprint | User: (CIT) Master` are on display.

7. With < or > select the user number and press `Enter`.
   `User: | No.` and `R. index finger` are on display.

8. With < or > select a finger and press `Enter`.
   `User: | No.` and `<<SCAN >>` are on display. The fingerprint sensor is activated as long as the brackets seem to be moving.

9. Put the finger onto the guiding and steadily move it downwards. Repeat doing this twice at least.
   After every successful scan '`x`' is displayed next to `User: No.` to indicate that you can put the finger onto the guiding again.
   `Bad image` is displayed in case the quality does not meet the set requirements.
   `No image` would be displayed if the sensor did not detect the finger.

No matching would be displayed if the sensor did recognize marks which do not match.
If four consecutive scans were unsuccessful, the registration of fingerprint data would be cancelled and would have to be started again.

10. Repeat the scanning process in case an error message is displayed.
Minu:XX Quali:XX | Please wait is on display in case the image quality meets the requirements. User: No.| Saved and
*One more finger? | *=yes *=no. are on display.*

11. With < and > select yes or no and press key Enter.
Depending on your choice, further messages might be displayed and you can scan another finger. Alarm finger | No finger would be displayed if the sensor had not detected a finger.

12. With < or > and Enter select an 'Alarm finger' or select No finger.
With an 'Alarm finger' silent alarm is triggered during lock opening.
User no. | Registered and afterwards
*Another code? | *= yes *=no are on display.*

13. Select *=yes, in case you want to register fingerprint code for further users and repeat performing steps 8 to 13.
Select *=no in order to end registering code.

You have successfully registered fingerprint code.

3.11.16 Deregistering Fingerprint Code

The lock master and the CIT master, as the case may be, can deregister fingerprint code of users.
Take care not to deregister Fingerprint codes necessary to arm / disarm an optional burglar alarm system (BAS).

1. Select menu Settings | Fingerprint.
For a detailed instruction, see paragraph 'Registering Fingerprint Code', steps 1-3. Fingerprint | Scan Test is on display.

2. With < or > select Deregister and press Enter.
Code entry and Lock 1, as the case may be, are on display.

3. Confirm with key Enter or, if necessary, select lock 2 or 3.
With the CIT function selected, Code entry | User: Master is on display. With < or > you can select CIT master and select Enter.
Without the CIT function selected, Code entry, Master, 0123456789 and Code: are on display.

4. Select the digits of the (CIT) master code with < and > and Enter.
(CIT) Master | Please wait and afterwards
Fingerprint | User: (CIT) Master are on display.

5. With < or > select the user number and press `Enter`.
   `User: No.` and `all fingers` will be on display, if user data are registered.
   `Fingerprint | OK` will be on display, if no user data are registered.

6. Press `Enter` in order to deregister all fingerprint data of the user or with < or > select a finger and press `Enter`.
   In order to cancel deregistering, press key `Clear`.

   In case you have deregistered user data of a finger, `Deregister | Deleted` will be on display.

   In case you have deregistered all fingerprint data of a user, `User: No. | Deleted` will be on display.

   In case you have deregistered user data of a finger defined as alarm finger, `Deregister | Alarm finger` and afterwards `New Alarm finger | no finger` will be on display. With < or > you can select another finger and by pressing `Enter` declare it the new alarm finger.

   `Another code? | *= yes *=no` are on display.

7. Select `*=yes` in case you want to deregister fingerprint code for further users and repeat performing steps 5 to 6.

   Select `*=no` in order to end deregistering code.

You have successfully deregistered fingerprint code.

3.11.17 Fingerprint User Display

The lock master and the CIT master, as the case may be, can display which fingerprint code is registered for users of a lock.

1. Select menu `Settings | Fingerprint`.
   For a detailed instruction, see paragraph 'Registering Fingerprint Code', steps 1-3. `Fingerprint | Scan Test` is on display.

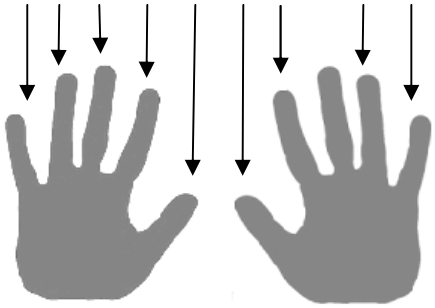
2. With key < or > select `User display` and press `Enter`.
   `Code entry` and `Lock 1`, as the case may be, are on display.

3. With key < or key > select the lock, if necessary, and press `Enter`.
   With the CIT function set, `Code entry` and `User: Master` are on display. With < or > you can select `CIT master` and press `Enter`.

   Without the CIT function set, `Code entry`, `Master`, `0123456789` and `Code:` are on display.

4. With < or > select the numbers of the master - / CIT master code and after each selection press `Enter` to confirm.
   `Please wait`, `(CIT) Master` or `User: No.` are on display.

5. With key< or key >, leaf through the user entries.
   In the first line `User: | XX` *and*
   in the second line `_ _*_ *_ _ a _ _ _.` *(example) are on display.*



Every underscore represents a finger.

* (asterisk): = registered finger
a : = alarm finger

6. End the display with key `Enter` or key `Clear`.
   `Fingerprint | User display` *are on display.*

You have successfully displayed fingerprint user data.

3.12 Service

Some Fingerprint submenus of menu `Service` have been added to the previous section 'Administering Users' above because important parameters for fingerprint code of users can be set with them.

3.12.1 Supplying Power in Case of Power Breakdown

Manufacturers of batteries offer fitting 9V block batteries like 6LR61 (alkaline type), 6F22 (zinc-carbon), 6AM6, 522.

Take an adapter cable (included in system delivery) and a loaded 9 V block battery. Access to FlatControl is required.

1. Connect adapter cable and battery Take notice of the different sizes of the sockets for negative and positive battery terminal.
2. Plug adapter cable into the socket at the bottom of the operating unit FlatControl.

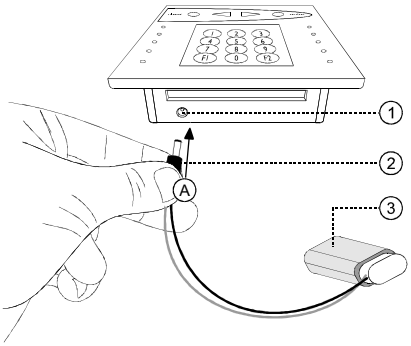
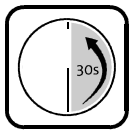


Fig. 23: Connect adapter cable to operating unit

1) Socket for emergency power supply
2) Plug of adapter cable
3) 9 Volt block battery

You successfully supply the system with power.

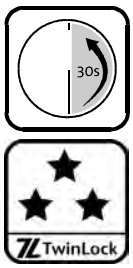
3.12.2 Displaying Status / Info about the System



1. Press key `Enter` and release it after a second.
   The system checks its status. The display shows date and time. .
2. With the menu keys < and > select `Status / Info` and press `Enter`.
   The display shows:
   - System Check
   - VdS class of the system
   - State of locks (open/middle pos. /closed)
   - State of system (unlocked / partly locked / locked)
   - State of an optional burglar alarm system (armed /disarmed)
   - Software version of operating unit
   - Software – and engine version of fingerprint module
   - Software version of locks
   - Software version of optional extension units TwinAlarm / TwinXT

You have successfully displayed status and software information about the system.

3.12.3 Service Reset



Via menu `Reset`, the system manager can undo the current settings and restore the default ex works settings.

Caution

System specific settings, included those concerning hardware and users, are deleted by resetting the system. After a Reset, only the lock master may be able to open locks.
Save the current configuration with the help of the optional software TwinComm USB or have it saved before carrying out a reset.

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.

2. With key < or key > select `Service` and press key `Enter`.
   `Service | Reset` *is on display.*

3. Confirm with `Enter`.
   `Code entry | System manager`, `0123456789`, *as the case may be, and* `Code` *are on display.*

4. Enter the system manager code.
   See paragraph 'Entering PIN Code' at the beginning of this chapter.
   `System manager | Please wait`, *and, afterwards,* `Reset` *and* `Delete finger? | *=yes *=no` *are on display.*
   If you select `*=yes`, *all fingerprint codes of all users will be deleted. See paragraph 'Deregistering Fingerprint Code' in this chapter in order to deregister / delete fingerprint code of selected users only.*

5. Confirm `*=no` with `Enter` or with key < or key > select `*=yes` and confirm with `Enter`.
   `System manager | Please wait`, *and, afterwards* `INITIALISING | DELETING EEPROM`, `OK`, `TwinLock` *and* `System Setup` *are on display.*

6. Confirm with `Enter`.
   `Language | 1 Deutsch` *is on display. By pressing* `Enter` *confirm the language or with key < or key > select another language.*

7. With < or > select `English`, for example, and press `Enter`.
   `English | Saved`, *as it may be, and* `System setup | New system` *are on display.*

8. With < or > select `Terminal change` and press `Enter`.
   `System setup | No. locks: 1` *is on display.*

9. With < or > select the number of locks which are part of the system and press `Enter`.
   `Serial no. | Lock 1`, `Code entry`, `System manager` and `Code:` are on display.

10. Enter the system manager code again.
    `Serial no. | Please wait` is on display.
    The serial number of the operating unit is saved in the lock.
    `Serial no. | Saved` is on display.

    With more than one locks in the system `Serial no. | Lock 2` and `Code entry | Manager` and `Code:` are on display.

11. If necessary, enter the manager code of lock 2, and afterwards, as the case may be, the manager code of lock 3.
    Default setting is that the manager code of all locks is the same as the ex works system manager code.
    `Serial no. | Please wait` is on display.
    The serial number of the operating unit is saved in the lock.
    `Serial no. | Saved` is on display.
    After the last lock, `Date / Time` and afterwards `Code entry | System manager` and `Code:` are on display.

12. Enter the system manager code again.
    Date and time are on display.

13. Press key `Enter` in order to set the time.
    If you press `Clear` two times, the time setting of the system will remain as it was and reset will be finished (see result after step 16).
    The cursor flashes at the first digit of the time setting.

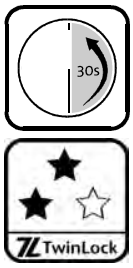
14. Enter the current time with < and > and `Enter`.
    The cursor flashes next to the day of the week.

15. With < and > select the first two letters of the current day of the week and press `Enter`.
    The cursor flashes at the first digit of the date setting.

16. Enter day, month and year.
    `Date / Time | Saved`,
    `Lock system | Registered` and
    `TwinLock BioPIN | 11.02.10` are on display.
    Also see paragraph 'Setting time and date'.

You have successfully deleted the former settings of the system and re-established the (default) settings ex works.

3.12.4 Motor Service



Lock masters can examine the bolt movement by moving the bolt of the lock step by step in both directions with menu `Motor service`.

Note

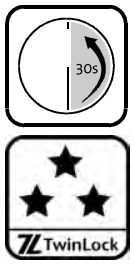
If 'automatic closing with door switch' is set via optional software TwinComm USB, the system will close the lock one minute after the motor steps described here have been performed.

Without automatic closing, the bolt will remain in the position reached via the last motor step.

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.
2. With key < or key > select `Service` and press key `Enter`.
   `Service | Reset` *is on display.*
3. With < or > select `Motor service` and press `Enter` again.
   `Service | Motor service` *is on display.*
4. Confirm with `Enter`.
   `Code entry | Lock 01` *is on display.*
5. With < or > select the lock, if necessary, and press `Enter`.
   `Code entry`, `Master`, `0123456789`, *as the case may be, and* `Code:` *are on display. See paragraph 'Entering PIN Code'.*
6. Enter the master code.
   `Motor service | <-= open | close =->` *is on display.*
7. With < or > select `open` or `close`.
   `Please wait` *is on display. The bolt drives in / out one motor step and stops.* `Step OK` *is on display.*
8. Repeat step 7 as often as necessary, in both directions, if required.

You have successfully driven the bolt of the lock step by step.

3.12.5 Registering a New Lock



Caution

Danger of bodily injuries for persons who do not perform the assembly professionally, as well as danger of damaging the system and causing malfunctions.
Make sure only trained specialists assemble and install the system.

Via menu `Service | Regist. new lock` register new locks only, which never have been part of a system before. This applies to changing a lock (`Change lock`) and to adding a lock (`New lock`).

In order to register locks that have already been addressed before, please proceed in the same way as when changing the operating unit. See instruction 'Service Reset' in this chapter and the Assembly Instructions.

Take a new lock, which has not been addressed yet.

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.

2. With key < or key > select `Service` and press key `Enter`.
   `Service | Reset` *is on display.*

3. With key < or > select `Regist. new lock` and press `Enter`.
   `Service | Regist. new lock` *is on display.*

4. Confirm with `Enter`.
   `Regist. new lock | New lock` *is on display.*

3.12.5.1 Additional New Lock

This paragraph is the sequel of 'Registering a New Lock' in case you register an additional new lock. Also see 'Changing a Lock' below.

5. Confirm `New lock` with `Enter`.
   `Code entry`, `system manager`, `0123456789` *and* `Code:` *are on display.*

6. Enter the system manager code.
   `Please wait`, `New lock`, `Lock 2/3` *and* `Insert bus cable` *are on display.*
   The lock number displayed is the number, which will be assigned to the new lock (number of formerly present locks + 1).

7. Connect the cable and afterwards confirm with `Enter`.
   `Serial no. | Please wait` *is on display. The serial number of the operating unit is saved in the lock.* `Serial no. | Saved` *is on display.*

   `Error com | Setup error` *would be on display if the 'new' lock had already been addressed.*

   `Date / Time | Saved`, `Lock |Registered` *and* `TwinLock BioPIN | 11.02.10` *are on display.*

You have registered the additional lock successfully.

3.12.5.2 Changing a Lock

This paragraph is the sequel of 'Registering a New Lock' in case you do not add a lock but change a lock. Also see 'Additional New Lock' above.

1. Perform steps 1-4 of instruction 'Registering a New Lock'.
   `Regist. new lock | New lock` *is on display.*

2. With < or > select `Change lock` and press `Enter`.
   `Change lock` *and* `Lock 1<` *are on display.*

3. With < or > select the lock to be replaced and press `Enter`.
   `Insert bus cable` *is on display.*

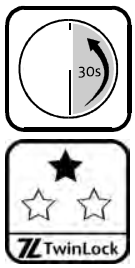
4. Connect the cable and afterwards confirm with `Enter`.
   `Error com | Setup error` *would be on display if the 'new' lock had already been addressed before.*
   `Serial no. | Lock 2/3` *and* `Code entry`*,*
   `System manager`*,* `0123456789` *and* `Code:` *are on display.*

5. Enter the system manager code.
   `Serial no. | Please wait` *is on display.*
   The serial number of the operating unit is saved in the lock.
   `Serial no.`*,* `Saved`*,*
   `Date / Time`*,* `Saved`*,*
   `Lock`*,* `Registered`*,*
   `TwinLock BioPIN` *and* `11.02.10` *are on display.*

You have successfully registered the new lock.

.

3.12.6 Locking the System despite Defect Bolt Work Contact



In case you have connected a circuit for a bolt work contact (via TwinXT or TwinAlarm), you still can lock the system once even with the bolt work contact being defect. Perform the steps described below and lock the system.

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.

2. With key < or key > select `Service` and press key `Enter`.
   `Service | Reset` *is on display.*

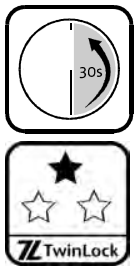
3. With < or > select `1x bolt work` and press `Enter`.
   `1x bolt work | *=yes *=no` *is on display.*

4. With < or > select `yes` and press `Enter`.
   `1x bolt work | Saved` *is on display. You can lock the system once even though the bolt work contact is defect.*

5. Close all locks in the system.
   Also see the instructions 'Close the Lock...'.
   The system is locked.

You have successfully locked the system despite a defect of the bolt work contact.

3.12.7 Fingerprint Status / Info



Via menu `Fingerprint | Status / Info`, users / operators can display the versions of software and engine of the fingerprint module.

1. Unlock the system by opening lock 1 or by opening all locks.
   See 'The System Status' at the beginning of this chapter.

2. With key < or key > select `Service` and press key `Enter`.
   `Service | Reset` *is on display.*

3. With key < or key > select `Fingerprint` and press key `Enter`.
   `Fingerprint | Status / Info` *is on display.*

4. Confirm with key `Enter`.
   The versions of the software and the engine of the fingerprint module are displayed.

You have successfully displayed version information about the fingerprint module.

3.12.8 Fingerprint: Displaying / Modifying Temperature

The system manager can display the operation temperature of the fingerprint sensor and, if necessary, modify it.
Range of values: Heating off, 18° – 50°, preset value: 40° Celsius.

Note

Danger of fingerprint scans of bad quality.
The proper temperature is an important prerequisite for the good quality of fingerprint data. After every modification of temperature, examine the quality.

1. Perform steps 1-3 of instruction 'Fingerprint Status / Info' above.
   `Fingerprint | Status / Info` *is on display.*
2. With key < or key > select `Temperature` and press key `Enter`.
   `Code entry | System manager`, `0123456789` *and* `Code` *are on display.*
3. With < or > select and with `Enter` confirm the digits of the code.
   `Temperature | 40° <` *is on display.*
4. Increase / Decrease the value with < or > and press `Enter`.
   `Temperature | Saved` *is on display.*

You have successfully displayed / modified the temperature.

4 Cleaning

Caution

Danger of short circuit of the electronic components.
Danger of damage to the system.
Note the following instructions on how to clean the system.

Clean the operating unit with very little, possibly mildly soapy water. Use a soaked, soft, clean and lint-free cloth. Do not use other means of cleaning equipment.

Clean all other components of your lock system TwinLock only if necessary. Use a dry, soft, clean and lint-free cloth only.
Wipe the surfaces exerting as little pressure as possible.

5 Trouble Shooting

5.1 Error Messages

Also see chapter ‘Operation’, paragraph ‘Configuration Import: Error Messages’.

`Arming error`

! TwinAlarm signals an error during arming the burglar alarm system (BAS): BAS cannot be armed because system is not locked.

✓ *Close the locks and repeat the procedure. Please contact technical support if the message is displayed again.*

`Authorisation`

`Close&Code` `Code card` `Disarm BAS` `Fingerprint` `No release!` `Open` `PIN code` `Service`

! Operators / users have not been authorised to perform the task they tried to perform. The system manager sets user authorisation in the User matrix of TwinComm USB. After one second, the missing kind of authorisation is on display. See below, ‘Code card’, ‘No release’...

✓ *Consult your system manager. Ask whether your authorisation can be extended via User matrix in optional software TwinComm USB.*

`Close&Code`

! Operator has not been authorised to close locks by entering his code.

✓ *Consult your system manager. See above.*

`Code card`

! Operator has not been authorised to use a code card.

✓ *Consult your system manager. See above.*

`Disarm BAS`

! Operator has not been authorised to disarm a burglar alarm system.

✓ *Consult your system manager. See above.*

`Fingerprint`

! Operator has not been authorised to enter fingerprint code.

✓ *Consult your system manager. See above.*

`No release!`

! Operator has not been authorised to enter code of any kind.

✓ *Consult your system manager. See above.*

`Open`

! Operator has not been authorised to open locks.

✓ *Consult your system manager. See above.*

`PIN code`

! Operator has not been authorised to enter PIN code.

✓ *Consult your system manager. See above.*

`Service`

! Operator has not been authorised to export protocols.

✓ *Consult your system manager. See above.*

`Bad image`

! Scanned fingerprint does not meet the set minimal requirements concerning the number of minutiae and / or the image quality.

✓ *Repeat scanning with different speed and pressure. Choose another finger, if possible.*

✓ *Check the set minimal requirements for fingerprints (min. minutiae and image quality) and modify them, if necessary.*

✓ *Please contact technical support, if the error message is displayed again.*

`Bio error`

! An error occurred during the execution of a fingerprint command.

✓ *Repeat the task you tried to accomplish. Please contact technical support if the message is displayed again.*

`Block period`

! When trying to open the lock
- a user has entered wrong code three times
- a block period of 90 minutes has been activated because at least one lock was closed during a terminal change
- a timer program, which blocks the lock, has been active.

✓ *Wait until the block period ends and open then.*

✓ *Check the protocol / Have the staff responsible for security check whether someone has tried to manipulate the system.*

`Bus A/B Receive`

`Bus A/B Transmit`

! A lock cannot be addressed via bus A / bus B. A bus cable connection might be plugged in incorrectly or the cable might be out of order.

✓ *If you cannot solve the problem, please contact technical support.*

`Codes identical!`

! PIN code, which should have been changed, has been repeated instead.

✓ *Change the PIN code.*

`Disarm code?`

! TwinAlarm signals an error during disarming the burglar alarm system (BAS): TwinAlarm cannot disarm BAS because no code authorised to disarm the BAS has been registered.

✓ *Activate alarm device TwinAlarm and register code at the lock while TwinAlarm is activated.*

`Disarming error`

! TwinAlarm signals an error during disarming the burglar alarm system (BAS): BAS cannot be disarmed because it does not acknowledge being disarmed.

✓ *Please contact staff with expert knowledge in alarm technology / technical support to have the connection to the BAS checked.*

`Error card`

! An error occurred in the communication between the operating unit and a chip card.

✓ *Repeat the task you tried to accomplish before the display of the message. Please contact technical support if the message is displayed again.*

`Error com`

`Bus A/B Transmit Bus A/B Receive`

! A lock cannot be addressed via bus A / bus B. A bus cable connection might be plugged in incorrectly or the cable might be out of order.

✓ *If you cannot solve the problem, please call for technical support.*

`Error com`

`Error Answer`

! An error occurred in the communication between the operating unit and another system component (a lock, for example). The operating unit has received a command it was not supposed to receive.

✓ *Software error. Please contact technical support.*

`Error card`

! An error occurred in the communication with the fingerprint module.

✓ *Repeat the task you tried to accomplish. Please contact technical support if the message is displayed again.*

`Error DMS No.`

! The lock TwinLock with the number displayed signals a general error.

✓ *Please contact technical support.*

`Error EEPROM AB / DMS / TM`

! Error when writing / reading the EEPROM of the bus systems (AB) / of lock TwinLock (DMS) / of the operating unit (TM for terminal).

✓ *Repeat the procedure, which caused the error message.*

✓ *If you cannot solve the problem, please contact technical support.*

`Error motor A`

`Error motor B`

! The lock bolt cannot be driven via bus A / bus B. Maybe the circuit board or the motor of the lock is out of order or the lock bolt cannot reach its end position due to a mechanical problem.

✓ *Please contact technical support.*

`Error RTC`

! The clock (real time clock) of the operating unit does not work properly.

✓ *Please contact technical support, if the error message is displayed again.*

`Error: Serial no.`

! Serial numbers in the operating unit and in the lock are not identical.

✓ *This message is on display after operating unit or lock have been replaced, but have not been changed according to the instructions. Sabotage is possible. Please contact the staff / persons responsible for security.*

`Error TwinAlarm`

! An error occurred in the communication with TwinAlarm.

✓ *Repeat the task you tried to carry out before the message was displayed. Please contact technical support if the message is displayed once more.*

`Finger timeout`

! Time for scanning is over. No finger has been moved across the sensor.

✓ *Repeat scanning. Put a finger onto the finger guide and steadily move the finger downwards.*

`Invalid card`

! The code card is invalid.

✓ *Check whether you have got a valid card. Please contact your system manager / the support if you do not have a valid card.*

`Invalid code | Block period`

! During an attempt at opening a lock, an operator has entered incorrect PIN code four times. Therefore a block time has been activated by the system. The block time, during which code entry is impossible, is prolonged by a minute after every time incorrect code is entered.

✓ *Wait until the block time has ended and enter your PIN code.*

✓ *Please contact your system manager / technical support, if you do not know the correct code.*

`Invalid input`

! A wrong or invalid input has been entered. Possibly code, date or time have been entered incorrectly or, with option 'Parallel code' or 'Dual code' selected, only one user (instead of two ones) has entered code.

✓ *Repeat the operation. Please contact technical support, if the error message is displayed again.*

`Just started or | was currentless`

! The system has been without power supply. The display of the message ends when a lock is opened.

✓ *Check whether date and time have been set properly.*

✓ *Check the protocol / have the staff responsible for security check whether someone has tried to manipulate the system.*

`Lock mid pos no.`

! Lock bolt is neither engaged nor disengaged but in middle position .

✓ *Check whether there is an obstacle in the way of the lock bolt.*

✓ *Check whether the lock can be opened and closed. If it cannot be opened or closed, please contact technical support.*

`Lock system`

! A lock master has made an attempt of deregistering a code without which the system could not be opened anymore.

✓ *Switch off option 'Dual code (4-eyes opening)' or 'Parallel code' or authorise more users to open the lock and register their code at the lock before de-registering the code in question.*

`! Manipulation !`

! Wrong code has been entered at least three times or a wrong finger has been scanned at least five times.

✓ *Read the protocol in order to see who has entered wrong code.*

`No card`

! No card has been inserted into the slot of the operating unit.

✓ *Insert a chip card into the card slot of the operating unit.*

`No fingerprint`

! No fingerprint code has been registered for the operator (user) for whom the message is displayed.

✓ *Consult your system administrator if fingerprint code is to be registered.*

`No image`

! Time for scanning is over. The sensor has not detected a fingerprint.

✓ *Repeat scanning. Please contact technical support, if the error message is displayed again.*

`No match`

! During a round of the registration of fingerprint code, different fingers have been scanned instead one finger being scanned repeatedly.

✓ *Move one finger along the sensor repeatedly until it is registered.*

`No release!`

! Opening is not possible. Lock has not been enabled via input contact RELEASE of TwinXT / TwinAlarm.

✓ *Check whether TwinXT / TwinAlarm are connected properly and whether the lock should be blocked or not. Please contact technical support, if the error message is displayed again.*

`No TwinAlarm!`

! Alarm device TwinAlarm has not been activated.

✓ *Make sure TwinAlarm is connected properly and is activated as well.*

`Not identified`

! Fingerprint has been scanned but could not be processed (recognised).

✓ *Repeat scanning with different speed and pressure. Choose another finger, if possible.*

✓ *Check security levels set for fingerprints and modify them, if necessary.*

✓ *Please contact technical support, if the error message is displayed again.*

`Lock system`

! A lock master has made an attempt of deregistering a code without which the system could not be opened any more.

✓ *Switch off option 'Dual code (4-eyes opening)' or 'Parallel code' or authorise more users to open the lock and register their code at the lock before deregistering the code in question.*

`Special days`

! The current date has been defined as a 'Special day', on which opening is not possible.

✓ *Wait until the 'Special day' ends.*

✓ *Open the lock (with authorisation 'quick open code').*

✓ *Check whether the date has been set properly at the operating unit and, if it is not the current date, change it.*

`Terminal change`

! The operating unit has been changed or reset. The display of the message ends at the time a lock is opened.

✓ *This message is displayed when a lock is opened or closed for the first time after the operating unit has been reset or changed. In this context the message does not require taking any measures.*

✓ *If the message is issued unexpectedly, somebody might have tried to manipulate the system. In this case, please contact the staff / persons responsible for security.*

`Timer p. aborted`

! Status message. Circuit TIMEOUT within the protected premises of the system is closed and suspends all active timer programs or a user with the authorisation 'quick open code' has opened a lock although a timer program was active.

✓ *Open the circuit TIMEOUT at terminals 30 and 31if you do not wish that active timer programs are suspended or*

✓ *Switch off authorisation 'quick open code' in the user matrix of TwinComm USB.*

`Trivial code`

! A user / an operator has entered code, which contains a row of ascending or descending numbers (12345…/ 76543..) .

✓ *Such code can be forbidden for security reasons. Enter another code.*

`Was currentless`

! The system has been without power supply. The display of the message ends at the time a lock is opened.

✓ *Check whether the date and time have been set properly.*

✓ *Check the protocol / have the staff / persons responsible for security check whether someone has tried to manipulate the system.*

`Weekly program`

! The current moment of time is not within a time slot defined for opening locks with the timer program 'Weekly program'.

✓ *Wait until a time slot for lock opening starts.*

✓ *Open the lock (with authorisation 'quick open code' in user matrix of TwinComm USB).*

✓ *Check whether the date has been set properly at the operating unit and, if it is not the current date, change it.*

`Wrong card`

! An operator has inserted a card of the wrong type into the slot at the operating unit, maybe a code card instead of a configuration card.

✓ *Select a card of the right type. Please contact your system manager / technical support, if you do not know what the expected card type is or if a card of that type is not available for you.*

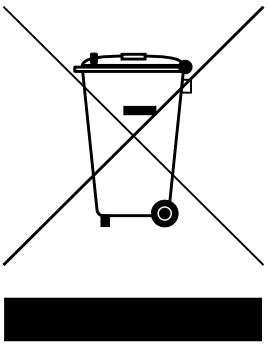
6 Support

INSYS MICROELECTRONICS GmbH
Business Unit Security Technologies
Waffnergasse 8
93047 Regensburg, Germany

Phone: +49(0)941/58 692 22
Fax: +49(0)941//56 34 71
Email: insys@insys-security.de
Internet: http://www.insys-security.de

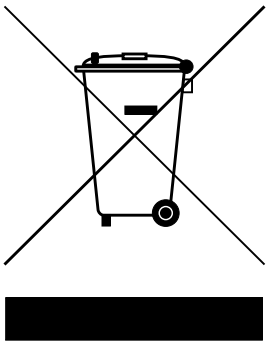
7 Disposal

Dispose of **plastic parts, electronic parts and cables** by taking them to a certified waste recycling company near to you where these materials are collected for later recycling and reuse or send them to the following address:



Frankenberg Metallhandel
Niederlassung Coburg
Gärtnersleite 8
D 96450 Coburg, Germany
Phone: +49(0) 9561 / 235 344
Fax: +49(0) 9561 / 235 319
E-mail: info@recycling-coburg.de
Internet: http://www.recycling-coburg.de

Please send the **locks**, marked ‘zur Entsorgung / to be disposed of’, to the following address:



INSYS MICROELECTRONICS GmbH
Waffnergasse 8
D 93047 Regensburg, Germany
Phone: +49(0) 941 / 586 92-22
Fax: +49(0) 941 / 563 471
E-mail: service@insys-security.de
Internet: http://www.insys-security.de

8 Glossary

Terms like **Alarm code**, which are printed in bold letters, are terms, which also are headings of entries in this glossary.

In order to make reading not unnecessarily difficult, only selected terms, which are important in the context they stand, are printed in bold letters. Also read the entries for these terms.

All entries are in alphabetical order.

Alarm code (for silent alarm)
The alarm code triggers **Silent alarm** and enables the lock master or (standard) users to perform the same tasks they can perform by entering their 'normal' PIN- or fingerprint code (of users and lock master).

Fingerprint code 'Alarm finger', see **Fingerprint**.

PIN code user or master code, in which the value set for 'alarm code' via software **TwinComm USB** is added to the last digit of the code.

If the last digit of your PIN code is '9', for example, enter '9 + the value for alarm code' as last digit. Should the result of this addition consist of a two-digit number, enter only the second digit as last code digit.

Example 9 + 1= 10. As last digit of the PIN code enter '0'.

Authorisation
Authorisation in the context of the lock system means the settings the **system manager** defines for users of the system in the **user matrix** of TwinComm USB. Also see chapter 'Operation', paragraph 'Authorising the Users'.

Authorisation to open a lock
Operators / users can open a lock only if

- the system manager has authorised them to do so (see chapter 'Operation', paragraph 'Authorising the Users') and
- the lock master has registered PIN - / fingerprint code and / or code cards for them at the lock (compatible with their authorisation) and
- no timer program prevents opening at the time they try to open the lock.

Optionally, system TwinLock can be configured in such a way that opening a safe is possible only for at least two persons who have to work together, optionally also according to a time schedule (also see **Dual code**, **Parallel code**).

Block period caused by terminal change with one lock closed
Time span of 90 minutes during which a lock is blocked. The block period is triggered after a terminal change has taken place during which at least one lock has been open.

Block period caused by input of wrong code
Time span of 1 minute and longer, as the case may be, during which a lock is blocked. The block period is triggered by repeated wrong code input by a user. The block period of one minute is prolonged in proportion to the frequency of wrong code input. Also see **Blocked period / Open period (timer program)**.

Blocked period / open period (timer program 1)
A blocked period is a time span of one day up to a year during which the system cannot be opened. Via software TwinComm USB (optional accessory), you can define up to three blocked periods. Every attempt at opening is cancelled during a blocked period. You can turn 'blocked periods' into 'open periods'. If you do that, opening will be impossible outside the 'open periods'. Before activating these options, make sure that time, day of week and date are set correctly. Also see **Block period caused by terminal change with one lock closed / ... by input of wrong code ...**.In all three cases the error message is 'Block period'.
Default setting: No blocked / open periods.

CIT function (2 user groups)

Caution

Without a CIT master sufficiently authorized, the CIT user group cannot be administered.
Authorise user 99 sufficiently (see chapter 'Operation', paragraphs 'Authorising the Users' and 'Operation with CIT Function Selected') before you select the CIT function.

With option 'CIT function' selected, the users of every lock are divided into two user groups. User no.99, who becomes CIT master administrates the new, second, user group. The former - one and only - user group decreases by the number of users of the second user group. The size of the groups can be set during configuration / modified via optional software TwinComm USB.

With or without CIT function, operation is the same for operators / users.

The lock master administers the first group of users (user no.01 - user no.XX-1). The new group of CIT users from user no.XX (= any number between 1 and 98 can be selected) to no.98 is administrated by user no.99, the CIT master.

Code
Code refers to secret data which operators / users have to transmit to the system before they can open (or close) locks or perform other tasks. Code can be transmitted in the form of PIN code or in the form of code cards.

Code card
Chip card of the type TwinLock code access. The card is to be inserted into the card slot of operating unit FlatControl. It is the carrier medium for code, an alternative or an optional complement to PIN - / fingerprint code input.

Code input
Two kinds of code input, which can also be combined, are possible:

- Entering PIN code (user code)
- Entering fingerprint code (in itself not sufficient for lock opening)
- Inserting a chip card (code card).

The system manager assigns all kinds or one / two of them to the operators / users and also defines whether a user may choose between them (boxes '1 of 3' and '2 of 3' in the user matrix). Also see 'Authorisation to Open a Lock'.

Code validity expiration
Optional, valid for PIN code. Setting range 00-12 months; 00 months = off

With this option selected, the registration date of every PIN code is checked every time a user tries to open a lock.

The system asks users to change their codes if they have been registered at least as long ago as the period set for code validity expiration lasts.

Deregister
The lock master has to register PIN codes and code cards at a lock in order to enable operators / users to open this lock with these codes and cards. Fingerprint codes have to be registered at locks, too.

If the lock master deregisters PIN code or a code card at a lock, the user to whom this code / card is assigned cannot open the lock with it.

If the lock master deregisters fingerprint code at a lock, the finger which corresponds to this code cannot be identified by the system anymore.

Dual code (4-Eyes Principle)
Optional setting which defines that opening locks is possible for two persons only (four-eye principle). Selected users / operators can be authorised to be able to open locks without a second person even when option 'Dual code' is selected.

Fingerprint, Fingerprint code
Entering fingerprint code in itself is not sufficient for opening locks but it can be a part of the authorisation of users.

For every lock the lock master (bearer of the master code of the lock), working together with the users, can register up to 10 biometric fingerprint codes for every user.

Before registering a fingerprint code for a user, minimal requirements for the user's fingerprints can be defined concerning the number of unique fingerprint attributes (**Minutiae**), the **Image quality** and the **Security level**. We recommend not to lower the default minimal requirement values for fingerprints.

One of the fingerprint codes of a user can be defined ‚alarm finger', which triggers **Silent alarm** when a lock is opened.

The bearer of the master code of a lock can display at the operating unit which fingers of which users are registered as fingerprint codes.

Forced sequence (FS)
Possibility of defining the order in which the locks of the system open and close.

If you program option 'Forced sequence' with software TwinComm USB, operators have to open lock 1 before they can open lock 2 and only with locks 1 and 2 open, lock 3 can be opened. The system is 'partly locked' (which corresponds to state 'locked' with option FS deactivated) when lock 1 has been opened. With all locks open, the system is 'unlocked', not protected.

Closing order: Lock 3 closes at first, afterwards lock 2 and the last lock to close is lock 1. Only after lock 1 has closed, the system is 'locked', protected.

Default setting: 'forced sequence' off.

Image quality
The value for minimal 'Image quality' of specific users can be set via menu Service / Fingerprint / Image quality.

Range of values: 20 – 99 (only the lower limit can be raised via TwinComm USB)

Default value: 30, should not be lowered.

The value for minimal ‚Image quality' is introduced to exclude templates of **Fingerprint code**, which do not contain the amount of information necessary to analyse the fingerprint and extract its attributes. A value of 60 represents excellent image quality. Values, which are much higher, cannot be achieved.

Possible reasons for low image quality:

- Finger movement over sensor too slow / too fast
- Finger pressure on sensor too high / too low / not constant
- wrong finger position
- finger too dry, too moist or dirty
- finger injuries like small cuts

In order to receive a high-quality image, move the finger over the sensor at constant speed while exerting very low pressure. Start with the fingertip on top of the guiding and move the finger downwards.

After every Scan test the image quality is on display at the operating unit. We recommend to have all users establish the average value for image quality which is characteristic of them and afterwards set the image quality to about 90% of this value (in menu Service/Fingerprint/Image quality).

Lock master

Bearer of the master code of a lock, who administers the codes (PIN codes and code cards) of the users / operators of the lock. Whether the lock master can open the lock depends on the settings of the system manager in the user matrix. Also see **CIT function**.

Manager code

Caution

The system is not protected with the ex works version of the system manager code.
Due to security reasons, change the ex works version of the code as soon as possible. Avoid using numbers, which might be guessed at by people with access to your personal data. Test entering new codes with the safe open.

For every lock there is exactly one manager code assigned to user no. 225 (lock manager). This code is stored in the lock and cannot be deregistered. With the manager code of lock 1, the 'system lock', you can modify system settings. Therefore this code also is called **system manager code**, in short system code. Ex works the manager code for locks of VdS class 2 is '111111' and for locks of class 3 it is '11111111'.

Master code

Caution

The system is not protected with the ex works version of the master code.
Due to security reasons, change the ex works version of the code as soon as possible. Avoid using numbers, which might be guessed at by people with access to your personal data. Test entering new codes with the safe open.

For every lock there is exactly one master code assigned to user no. 00 (lock master). This code is stored in the lock and cannot be deregistered. With it, lock users (operators) can be administered. Ex works the master code for locks of VdS class 2 is '123456' and for locks of class 3 it is '12345678'. Via user matrix of the optional PC software TwinComm USB the **system manager** can define whether the bearer of the master code can open locks.

Minutiae
Unique attributes of a fingerprint. A minimal number of these attributes, which a fingerprint is to have, can be set via menu Service/Fingerprint/Min. Minutiae.

Range of values: 09 - 50 (only the lower limit can be raised)

Default value: 18

With value ‚18' set, during the registration of fingerprint code every attempt at registering fingerprint code is rejected if the sensor does not detect at least 18 minutiae.

The number of minutiae of individual fingertips varies very much. We recommend to have users / operators find out for themselves via menu Scan Test how many minutiae their fingers feature. Afterwards, the lock master can subtract about 3-4 from the lowest value of a finger to be registered and enter the resulting numbers as lower limits for the individual users' fingerprint code (in menu Service / Fingerprint / Min. Minutiae).

Open period
See **Blocked Period / Open Period (Timer Program)**.

Parallel code
Option, which can be selected only with systems with at least two locks. The first operator to open can open lock 1, 2 or 3. The second operator to open can open any of the two locks still closed. The third operator to open opens the last closed lock. For each of the three operators identical PIN code has to be registered at all three locks (operator 1 has '101010' registered at lock 1, 2 and 3, operator 2 has '202020' registered at lock 1, 2 and 3 and operator 3 has registered '303030' at lock 1,2 and 3, for example).

Can be combined with '**Forced sequence**'. With two locks in the system, one operator can open locks single-handedly during a '**Part Lock Time**'.

If you select this option via software TwinComm USB, the software will switch off option 'Dual Code' automatically.

Part lock(ed) time (3 periods per day)
Before activating a part lock time, make sure that time, day of week and date are set correctly. For systems with two locks, you can define three periods of 'Part lock time' per day via software TwinComm USB (optional accessory). During the periods of part lock time only lock 2 closes, lock 1 remains open. While a period lasts, every attempt at closing lock 1 is cancelled.

Default setting: 'Part lock time' off.

In order to close lock 1 in spite of active 'Part lock time':

Press key `ENTER` while `Close | lock 1 Partly locked!` is displayed. Lock 1 is closed, 'Part lock time' is suspended for this single closing process.

You can combine option 'Part lock time' with option 'Automatic closing with door switch'. If you do that, lock 1 will stay open during part lock time and will be closed when the part lock time ends.

PIN code
Sequence of numerical digits known only by the operator or by the lock master, too, which the operator uses for his authentication, an alternative or an optional complement to **code card** / **Fingerprint code**.

Protocol (event log)
All important events are logged chronologically with date and time. The protocol can be exported, depending on the system version also online. Devices and operators involved in an event are listed. The latest 3000 events are logged. Events are programming processes, system errors, important status messages and attempted acts of sabotage and manipulation. The complete event log memory can be transferred to chip card TwinCard configuration II and displayed as well as printed via PC software TwinComm USB.

Power breakdown
Power is supplied to the system via a power pack connected to TwinConnect. In order to be able to open and close locks even when a power breakdown has occurred, connect a 9 V battery (alkaline or zinc-carbon type) to the operating unit. Plug the adapter cable into the socket at the bottom of the operating unit. See paragraph 'Supplying Power in Case of Power Breakdown'.

Quick open code
Box in the user matrix of optional software TwinComm USB. If ticked (AE checked) for users / operators, these operators can open the lock without (timed) delay even despite timer programs assigned to them.

The operators can open immediately only in case all other boxes necessary for authorisation have been ticked fort hem as well and in case their PIN code / code card has been registered at the lock.

Real-time clock
A real-time clock with an alternative energy source provides system date and time, which are sustained even in case of a power failure lasting several days.

If the operating unit is separated from power supply for a longer period, it will be necessary to enter the proper date and time after that. Automatic clock change in spring and autumn (Daylight Saving Time) is default setting, which can be changed on tab 'Settings' of software TwinComm USB.

Register
The lock master has to register PIN codes and code cards at a lock in order to enable operators / users to open the lock with these codes and cards. Fingerprint code can be registered by users accompanied by the lock master.

Release time
Via tab 'Settings' of optional software TwinComm USB, you can define a release time ranging from 1 to 15 minutes for every lock.

Also via TwinComm USB, you can program an **Unlocking (time) delay** for locks, during which a lock remains closed even after an operator has entered code.

With option 'Release time' selected (via TwinComm USB), an operator has to enter his code a second time after the unlocking delay has ended and during the time span defined as release time. Only after this second code input the lock opens.

With option 'Release time' not selected, the lock opens as soon as the delay ends.

Security level
The parameter ‚Security level' defines the kind of similarity required to make the system interpret scanned fingerprint data as being identical with registered fingerprint code. As this value determines whether a person is identified, it has direct impact on the security of the system. The amount of similarity of scans is

displayed as ‘Matching’ after the second round of scanning (via menu Scan test). From the value displayed subtract about 10-15 (tolerance) and enter the result as ‚Security level’ for users via menu Service / Fingerprint / Security level.

Range of values: 30 - 99

Default value: 60, general minimal requirement (TwinComm USB): 40

Security Level	False Rejection Rate	False Acceptance Rate
45	<2%	0.0001
50	<3%	0.00001
60	<4%	0.000001

The table above makes it evident that the higher the value for ‚Security level’, the lower the probability of false identification and the higher the probability of false rejection.

With a security level of 45 less than 2% of all fingerprints which should match are interpreted as being not identical and the fingerprint of a person not authorised is interpreted as being identical with a registered fingerprint with a probability of 0,01 %.

Service

1) Menu of the display of the operating unit FlatControl for service functions
2) Box in the user matrix of PC software TwinComm USB. If the system manager ticks (AE: checks) the box ‘Service‘ for users / operators, these operators can export the event log via chip card from the system and display and print and save it with software TwinComm USB.

Silent alarm

Only with PIN code input, not with code card. If threatened, operators can trigger silent alarm by entering a special ‘**alarm code**’ when opening a lock. The system performs in the same way as it does in the case of a ‘normal’ opening with the only difference that additionally a silent alarm signal is sent to the burglar alarm system.

Special days

Caution

Danger of defining special days unintentionally.
Unexpectedly opening locks is impossible.
Take care not to mark holidays like Easter, which do not take place at the same date every year, as ‘annually recurring’.

Special days are days on which opening locks is impossible during the whole day. You can define up to 30 special days in a year via optional software TwinComm USB. Every attempt at opening a lock on a special day is aborted. ‘Special days’ can be marked as ‘annually recurring’ (on the same date).

Before programming **timer program** ‘Special days’, make sure that time, day of the week and date are set correctly.

Default setting: Special days Off

System manager

Bearer of the system manager code, with which the system can be configured. The system manager cannot open and close locks.

System manager code (=manager code of lock 1)

Caution
With the system manager code in ex works version, your system is not protected. Change ex works code as soon as possible. Never use series of numbers corresponding with personal data. Test entering new PIN codes with the safe open.

The system manager code, in short the system code, authorises to configure the system via the operation unit. It is stored in lock 1 of the system and is assigned to user no. 225.
Ex works this code is '111111' (with systems of VdS class 2) or '11111111' (with systems of VdS class 3).

Timer program
The time span, during which locks can be opened, can be restricted in various ways. Also see the entries **Special days**, **Blocked period**, **Part lock time** and **Weekly program**. Timer programs / Blocked periods can be aborted (suspended) by privileged users. Also see '**Timer program abortion**' and '**Quick open code**'.

Timer program abortion
A person within the protected premises can press a button inside the safe which overrules active **timer programs** (weekly program, special days, block period or part time lock)and makes it possible to open the lock from the outside by user authentication (usually code input). After one opening process, the timer programs are activated automatically. Such a button can be connected via TwinAlarm only and not via extension unit TwinXT.

Even without TwinAlarm, users can abort active timer programs if they have been authorised to open in spite of timer programs by the system manager (box 'quick open code' in user matrix of TwinComm USB). Also see '**Quick open code**'.

TwinComm USB
Optional accessory. Configuring set, software for system TwinLock. Every system is configured with TwinComm USB after installation. The user matrix of system TwinLock, in which the basic authorisation for operators is defined, is part of the software TwinComm USB.

Unlocking (Time) Delay
Via TwinComm USB, you can program an **Unlocking (time) delay** for locks ranging from 1 to 99 minutes, during which a lock remains closed even after an operator has entered code. Also see option '**Release time**'.

With option 'Release time' not selected, the lock opens as soon as the delay ends.

User matrix
Tab of graphical user interface of software TwinComm USB, on which the authorisation of operators is defined. See chapter 'Operation', paragraph 'Authorising the Users'.

Weekly program
Via optional software TwinComm USB you can install up to 5 weekly programs with freely definable opening periods for every day of the week. Via user matrix, you can assign the programs to users individually. With activated weekly program(s), every opening process is cancelled which is not within a defined opening period. Before activating a weekly program, make sure that time and date are set correctly.

Default setting: no weekly programs.

9 Appendix

9.1 Index of Keywords

1 of 3 86
ACE 18
Adapter Cable 69
Affirm with Enter Key 25
Alarm
  Alarm Code 37
  Silent Alarm 37
  Switch on / - off Alarm Devices 44
Alarm Code 85
Assembly Instructions 6
Authorisation 77, 85
  1 of 3 29
  2-eyes 29
  Boxes 27
  Quick Open Code 29
  Release 29
  Service 29
  User Matrix 27
  Weekly Program 29
Base System 9
  Base System 1.1 10
  Base System 2.1 11
  Base System 3.2 12
Battery 69
Block Period
  Terminal Change 85
  Timer Program 86
  Wrong Code 85
Blocking Device 18
Bolt Mechanism Contact 18
Burglar Alarm System 14, 16, 41
  Arm 42
  Disarm 41
Bus Distributor 17
Cancel with Clear Key 25
Chip card
  Icon 8
  Insert 32
CIT
  CIT Function 86
  CIT Master 34
  CIT Master Code 52
  Switch on / - off CIT Function 44
Cleaning 76
Clear Key 25
Clock Change 23
Code 86
  Dual Code 38
  Mnemonic 20
  Parallel Code 40
  Physical 20
  Validity Expiration 86
Code Card 19, 32
  Deregister 58
  Register 57
  User Display 59
Comfort System 9
  Comfort System 1 13
  Comfort System 2 15
Configuration
  Export 49
  Import 46
  TwinComm USB 27
Date Setting 43
Default Settings, Restore 70
Deregister 87
Disposal 84
Door Switch 23
Dual Code 87
Enter Key 25
Error Messages 77
  Configuration 47
Fingerprint 87
  Image Quality 63, 87
  Minutiae 62
  Scan Test 61, 75
  Security Level 64, 91
  Survey 60
  User Display 67
Fingerprint Code
  Deregister 66
  Enter 36
  Register 65
FlatControl 17
  Cleaning 76
  Icon 7
Forced Sequence 87
Icons 7
Import Configuration 46
Language
  Import 50
  Select 49
Lock
  Additional Lock 73
  Bolt in Mid Position 80

Change ... 74
Close ... 41
Close Automatically ... 42
Close with Code Input ... 41
Motor Step ... 72
Open with Code Card ... 35
Open with PIN Code ... 35
Register ... 73
TwinLock ... 17
Lock Master ... 88
Manager Code ... 88
Icon ... 8
Manual ... 6
Master Code ... 88
Change ... 52
Ex Works ... 32
Icon ... 8
Menu Keys ... 25
Minutiae ... 89
Motor Service ... 72
Operating Instructions ... 8
Keys ... 8
Materials ... 8
Objective ... 8
Preconditions ... 8
Tools ... 8
Operating Unit ... 25
Menu Navigation ... 30
Parallel Code ... 89
Part Lock Time ... 89
PIN Code ... 89
Change ... 54
Deregister ... 55
Icon ... 7
Personal Data ... 31
Register ... 53
Trivial Code ... 82
User Display ... 56
Power Breakdown ... 90
Power Supply ... 69
Protected Premises Icon ... 8
Protocol ... 90
Export ... 45
Print ... 45
Qualification ... 6
Quick Open Code ... 90
Quick Reference Guide ... 6
Real-Time Clock ... 90
Register ... 90
Release Time ... 39, 90
Safety Warnings ... 7
Security Level ... 90
Service ... 91
Authorisation ... 91
Menu ... 91
Reset ... 70
Settings ... 26
Reset ... 71
Silent Alarm ... 91
Alarm Code ... 85
Software ... 23
Version Display ... 69
Special Days ... 91
System ... 9
Lock Despite Defect Contact ... 75
System Manager ... 91
System Manager Code
Change ... 51
Ex Works ... 32
Icon ... 8
Table of Contents ... 3
Text Marks ... 7
Time Setting ... 43
Timer Program ... 24, 92
Weekly Program ... 24
Blocked Periods ... 24
Part Lock Periods ... 24
Special Days ... 24
Tools Icon ... 7
Trademarks ... 2
TwinAlarm ... 18
Register Code ... 53
TwinCard
code access ... 8, 19, 32
configuration II ... 8, 19, 45, 46
language ... 8, 19, 50
TwinComm USB ... 23, 27, 46, 92
User Matrix ... 92
TwinConnect ... 17
TwinXT ... 18
Unlocking Delay ... 39, 90, 92
Release Time ... 39
Use ... 9
Intended Use ... 24
User Matrix ... 85
Authorisation ... 27, 28
VdS Class ... 31
VdS Schadenverhütung ... 6
Weekly Program ... 93

9.2 Table of Figures

Fig. 1: System architecture of Base System 1.1 10
Fig. 2: System architecture of Base System 2.1 11
Fig. 3: System architecture of Base System 3.2 12
Fig. 4: System architecture of Comfort System 1 without BAS 13
Fig. 5: System architecture of Comfort System 1 with BAS 14
Fig. 6: System architecture of Comfort System 2 without BAS 15
Fig. 7: System architecture of Comfort System 2 with BAS 16
Fig. 8: Operating Unit FlatControl BioPIN 17
Fig. 9: Lock TwinLock 17
Fig. 10: Bus distributor TwinConnect 17
Fig. 11: Blocking device TwinXT 18
Fig. 12: Ancillary control equipment (ACE) TwinAlarm 18
Fig. 13: Icon 'TwinCard code access' 19
Fig. 14: Icon 'TwinCard language' 19
Fig. 15: Icon 'TwinCard configuration II' 19
Fig. 16: Survey: codes in the system 20
Fig. 17: PC software TwinComm USB (accessory) 23
Fig. 18: Operating unit FlatControl BioPIN 25
Fig. 19: Start page of PC software TwinComm USB (accessory) 27
Fig. 20: Section of user matrix in TwinComm USB 28
Fig. 21: Card and card slot of FlatControl BioPIN 33
Fig. 22: Operating unit with guiding for fingers 60
Fig. 23: Connect adapter cable to operating unit 69

9.3 Document Revision History

Version	Date	Modification	Name
1.03.A	11.02.10	First English edition; update illustrations	MR
1.03B	24.03.10	Update TwinConnect	MR

!!! Errors excepted!!!

9.4 Notes